Guia do Desenvolvedor

AWS Config

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: Guia do Desenvolvedor

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é AWS Config? ... 1
Considerações ... 1
Maneiras de usar AWS Config ... 1
Administração de recursos ... 2
Auditoria e Compatibilidade ... 2
Gerenciar e solucionar problemas de alteração de configuração ... 2
Análise de segurança ... 2
Soluções para parceiros ... 3
Atributos ... 3
Como AWS Config funciona ... 4
Descoberta de recursos ... 5
Acompanhamento de recursos ... 5
Entrega de itens de configuração ... 6
Controle o acesso ao AWS Config ... 9
Conceitos ... 10
AWS Config Interfaces ... 11
Gerenciamento de recursos ... 12
Gravador de configuração ... 12
Nome do canal de entrega ... 6
AWS Config Regras ... 14
Pacotes de conformidade ... 17
Agregadores ... 18
Suporte regional ... 19
Service Limits ... 24
AWS Integrações de serviços ... 26
AWS Organizations ... 26
AWS Control Tower ... 27
AWS CloudTrail ... 27
AWS Security Hub ... 27
AWS Audit Manager ... 27
AWS Systems Manager ... 28
AWS Firewall Manager ... 28
Hosts dedicados do Amazon EC2 ... 28
Application Load Balancers ... 29

AWS CodeBuild ... 29
AWS X-Ray ... 29
AWS Service Management Connector ... 30
Amazon API Gateway ... 30
Informações complementares ... 30
AWS Kits de desenvolvimento de software para AWS Config ... 31
Conceitos básicos ... 33
Inscrevendo-se para AWS ... 33
Inscreva-se para um Conta da AWS ... 33
Criar um usuário com acesso administrativo ... 34
Maneiras de começar com AWS Config ... 35
Configuração AWS Config (console) ... 35
Configuração ... 35
Configuração com um clique ... 36
Configuração manual ... 40
Configurando AWS Config (AWS CLI) ... 47
Configuração ... 47
Pré-requisitos ... 48
Começando AWS Config ... 109
Verificação ... 120
Trabalhando com AWS SDKs ... 122
Gravador de configuração ... 124
Gerenciar o gravador de configurações (Console) ... 124
Gerenciar o gravador de configurações (AWS CLI) ... 125
Detecção de desvio para o gravador de configuração ... 129
Nome do canal de entrega ... 130
Terminologia ... 131
Atualizar o canal de entrega ... 132
Renomear o canal de entrega ... 136
Componentes de um item de configuração ... 137
Fornecer snapshot de configuração ... 139
Entregando instantâneos de configuração ... 139
Exemplo de instantâneo de configuração de AWS Config ... 140
Verificar o status de entrega ... 145
Visualizar o snapshot de configuração no bucket do Amazon S3 ... 146
Exemplo de notificações ... 147

Exemplos de notificações de alteração de item de configuração 148
Exemplo de notificação de entrega de histórico de configuração 163
Exemplo de notificação de entrega de snapshot de configuração iniciada 164
Exemplo de notificação de entrega de snapshot de configuração 165
Exemplo de notificação de alteração de compatibilidade 165
Exemplo de notificação de avaliação de regras iniciada 169
Exemplo de notificação de alteração de item de configuração superdimensionado 170
Exemplo de notificação de falha na entrega 171
Gerenciamento de recursos 173
AWS Config Painel de controle 173
Inventário de conformidade e recursos 174
AWS Config Métricas de uso e sucesso 176
Tipos de recursos compatíveis 178
Amazon AppStream 180
Amazon AppFlow 180
..... 180
Amazon API Gateway 181
Amazon Athena 181
Amazon CloudFront 182
Amazon CloudWatch 183
Amazon CodeGuru 183
Amazon Cognito 184
Amazon Connect 184
Amazon Detective 185
Amazon DynamoDB 185
Amazon EC2 186
Amazon ECR 194
Amazon ECS 194
Amazon EFS 195
Amazon EKS 195
Amazon EMR 196
Amazon EventBridge 196
Amazon Forecast 197
Amazon Fraud Detector 198
Amazon GuardDuty 199
Amazon Inspector 199

Amazon IVS 199
Amazon Keyspaces 200
OpenSearch Serviço Amazon 200
Amazon Personalize 201
Amazon Pinpoint 202
Amazon QLDB 203
Amazon Kendra 203
Amazon Kinesis 203
Amazon Lex 204
Amazon Lightsail 204
Amazon Lookout for Metrics 205
Amazon Lookout for Vision 205
Amazon Managed Grafana 206
Amazon Managed Service para Prometheus 206
Amazon MemoryDB para Redis 206
Amazon MQ 206
Amazon MSK 207
Amazon Redshift 207
Amazon RDS 209
Amazon Route 53 211
Amazon SageMaker 212
Amazon SES 213
Amazon SNS 214
Amazon SQS 214
Amazon S3 214
Amazon WorkSpaces 216
AWS Amplify 217
AWS AppConfig 217
AWS App Runner 218
AWS App Mesh 218
AWS AppSync 219
AWS Audit Manager 220
AWS Auto Scaling 220
AWS Backup 221
AWS Batch 222
AWS Budgets 222

AWS Certificate Manager 223
AWS CloudFormation 223
AWS CloudTrail 223
AWS Cloud9 224
AWS Cloud Map 224
AWS CodeArtifact 225
AWS CodeBuild 225
AWS CodeDeploy 225
AWS CodePipeline 226
AWS Config 227
AWS DMS 228
AWS DataSync 228
AWS Device Farm 230
AWS Elastic Beanstalk 230
AWS FIS 231
AWS Global Accelerator 231
AWS Glue 232
AWS Ground Station 232
AWS HealthLake 233
AWS IAM 233
AWS IoT 235
AWS KMS 238
AWS Lambda 239
AWS Mainframe Modernization 239
AWS Network Firewall 239
AWS Network Manager 240
AWS Panorama 241
AWS Private CA 242
AWS Resilience Hub 242
Explorador de recursos da AWS 243
AWS RoboMaker 243
AWS Signer 244
AWS Secrets Manager 244
AWS Service Catalog 244
AWS Shield 245
AWS Step Functions 245

AWS Systems Manager ... 246
AWS Transfer Family ... 247
AWS WAF ... 247
AWS X-Ray ... 249
Elastic Load Balancing ... 250
MediaConnect ... 251
MediaPackage ... 251
MediaTailor ... 252
Cobertura de recursos por região e disponibilidade ... 252
América do Norte e América do Sul ... 252
Europa ... 323
Ásia-Pacífico ... 371
China ... 419
África e Oriente Médio ... 453
GovCloud ... 501
AWS Recursos de gravação ... 545
Considerações ... 545
Recursos regionais e globais ... 546
Gravar recursos (console) ... 549
Recursos de gravação (AWS CLI) ... 553
Frequência de gravação ... 569
Interromper a gravação ... 570
Recursos não gravados ... 570
AWS Config Regras e tipos de recursos globais ... 571
Gravar recursos de terceiros ... 573
Etapa 1: Configurar o ambiente de desenvolvimento ... 573
Etapa 2: Modelar seu recurso ... 574
Etapa 3: gerar artefatos ... 576
Etapa 4: registrar o recurso ... 576
Etapa 5: publicar a configuração do recurso ... 576
Registre e exclua um estado de configuração para recursos de terceiros usando AWS CLI ... 577
Gerenciar um estado de configuração para os tipos de recursos de terceiros usando APIs ... 580
Configurações do software de gravação ... 580
Visualizar recursos da gravados ... 583
Inventário de recursos ... 583

Informações de conformidade e resultados da avaliação ... 585
Histórico de configuração e conformidade ... 598
Marcar os recursos do ... 607
Restrições relacionadas à marcação ... 608
Gerenciar tags com ações de API do AWS Config ... 608
AWS Regras de configuração ... 610
Considerações sobre custos ... 611
Suporte regional ... 612
Componentes de uma regra ... 619
Metadados da regra ... 619
Estrutura da regra ... 621
Modo de avaliação ... 640
Tipos de trigger ... 640
Modos de avaliação ... 641
Avaliações da regra ... 645
Regras gerenciadas ... 646
Considerações sobre custos ... 611
Tipos de trigger ... 647
Modos de avaliação ... 648
Lista de regras gerenciadas do ... 649
Lista de regras gerenciadas por modo de avaliação ... 952
Lista de regras gerenciadas por tipo de acionador ... 968
Lista de regras gerenciadas por disponibilidade da região ... 983
Regras vinculadas ao serviço ... 1320
Criação de regras gerenciadas comAWS CloudFormation modelos ... 1321
Regras personalizadas ... 1323
Regras de política personalizadas ... 1323
Regras personalizadas do Lambda ... 1324
Considerações sobre custos ... 611
Tipos de trigger ... 1325
Modos de avaliação ... 1326
Gerenciar recursos excluídos ... 1327
Criar regras de política personalizadas ... 1329
Criação de regras personalizadas do Lambda ... 1332
Adicionar, atualizar e excluir regras ... 1366
Usar o console ... 1366

Usando os AWS SDKs ... 1372
Usar o Security Hub ... 1385
Avaliar recursos com regras ... 1385
Exclusão de resultados de avaliação ... 1390
Excluindo resultados da avaliação (console) ... 1390
Excluindo resultados da avaliação (CLI) ... 1390
Excluindo resultados da avaliação (API) ... 1391
Gerenciar regras organizacionais ... 1391
Considerações ... 1391
Implantação ... 1392
Suporte regional ... 1393
Correção ... 1396
Pré-requisito ... 1396
Configurar a correção manual (console) ... 1397
Configurar a correção automática (console) ... 1398
Excluir ação de correção (console) ... 1399
Gerenciar remediação (API) ... 1400
Suporte regional ... 1401
Solução de problemas ... 1404
Pacotes de conformidade ... 1407
Pré-requisitos ... 1407
Comece a AWS Config gravar ... 1408
Pré-requisitos para usar um pacote de conformidade com correção ... 1408
Pré-requisitos para usar um pacote de conformidade com uma ou mais regras AWS Config ... 1409
Pré-requisitos para pacotes de conformidade da organização ... 1412
Suporte regional ... 1413
Verificações de processo ... 1419
Exemplo de modelo de pacote de conformidade para criar verificações de processo ... 1420
Inclua verificações de processo em um pacote de conformidade ... 1420
Alterar o status de conformidade de uma verificação de processo ... 1421
Exibir e editar a verificação do processo (console) ... 1422
Exemplos de modelos de pacote de conformidade ... 1423
AWSPacote de conformidade Control Tower Detective Guardrails ... 1427
Práticas operacionais recomendadas para workloads de materiais do CCIG 2.0 da ABS ... 1427
Práticas recomendadas operacionais para workloads padrão do CCIG da ABS 2.0 ... 1659

Práticas recomendadas operacionais para o ACSC Essential 8 1831
Práticas recomendadas operacionais para o ISM do ACSC 1858
Práticas recomendadas operacionais para IA e ML 1997
Práticas recomendadas operacionais para o Amazon API Gateway 1998
Melhores práticas operacionais para a Amazon CloudWatch 1998
Melhores práticas operacionais para o Amazon DynamoDB 1998
Melhores práticas operacionais para o Amazon S3 1998
Práticas recomendadas operacionais do CPG 234 da APRA 1998
Práticas recomendadas operacionais para o gerenciamento de ativos 2238
Práticas recomendadas operacionais para o AWS Backup 2238
Melhores práticas operacionais para gerenciamento de AWS identidade e acesso 2239
Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework 2239
Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework 2307
Práticas recomendadas operacionais para BCP e DR 2491
Práticas recomendadas operacionais para o BNM RMit 2492
Práticas recomendadas operacionais para o perfil de controle de nuvem médio do Canadian Centre for Cyber Security (CCCS) 2837
Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1 ... 4484
Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2 ... 4528
Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG1 4587
Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG2 4692
Práticas recomendadas operacionais para CIS Critical Security Controls v8 IG3 4877
Práticas recomendadas operacionais para o CIS Top 20 5079
Prática recomendadas operacionais para o CISA Cyber Essentials 5162
Práticas recomendadas operacionais para Serviços de Informação da Justiça Criminal (CJIS) 5382
Práticas recomendadas operacionais para a CMMC Nível 1 5525
Práticas recomendadas operacionais para a CMMC Nível 2 5655
Práticas recomendadas operacionais para a CMMC Nível 3 5979
Práticas recomendadas operacionais para a CMMC Nível 4 6456
Práticas recomendadas operacionais para a CMMC Nível 5 6972
Práticas recomendadas operacionais para o CMMC 2.0 Nível 1 7559
Práticas recomendadas operacionais para a CMMC 2.0 Nível 2 7688
Práticas recomendadas operacionais para serviços de computação 8133

Práticas recomendadas operacionais para a resiliência de dados 8134
Práticas recomendadas operacionais para serviços de bancos de dados 8134
Práticas recomendadas operacionais para o data lakes e os serviços de análise 8134
Práticas recomendadas operacionais para o DevOps 8135
Práticas recomendadas operacionais para o EC2 8135
Práticas recomendadas operacionais para criptografia e gerenciamento de chaves 8135
Práticas recomendadas operacionais do Guia de segurança cibernética da ENISA para PMEs 8135
Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Low 8315
Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Medium 8429
Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) High 8555
Operational Best Practices for FDA Title 21 CFR Part 11 8690
Práticas recomendadas operacionais para o FedRAMP (Baixo) 9106
Operational Best Practices for FedRAMP(Moderate) 9399
Operational Best Practices for FFIEC 10009
Práticas recomendadas operacionais do Catálogo de Critérios de Conformidade de Computação em Nuvem da Alemanha (C5) 10255
Práticas recomendadas operacionais para o Gramm Leach Bliley Act (GLBA) 10347
Práticas recomendadas operacionais para o Anexo 11 da GxP da UE 10406
Operational Best Practices for HIPAA Security 10583
Práticas recomendadas operacionais para o IRS 1075 11135
Práticas recomendadas operacionais para o K-ISMS 11375
Práticas recomendadas operacionais para o balanceamento de carga 11465
Práticas recomendadas operacionais para o Registro 11466
Práticas recomendadas operacionais para serviços de gerenciamento e governança 11466
Práticas recomendadas operacionais para o Aviso 655 do MAS 11466
Práticas recomendadas operacionais para as TRMG da MAS 11508
Práticas recomendadas operacionais para o monitoramento 11748
Práticas recomendadas de operação para as TRMG do NBC 11749
Práticas recomendadas operacionais para o NERC CIP BCSI 12307
Práticas recomendadas operacionais para o NCSC Cloud Security Principles 12379
Práticas recomendadas operacionais para a Estrutura de Avaliação Cibernética do NCSC 12501
Práticas recomendadas operacionais para serviços de rede e entrega de conteúdo 12702

Práticas recomendadas operacionais para o NIST 800-53 rev 4 12702
Práticas recomendadas de operação do NIST 800-53 rev 5 13045
Práticas recomendadas operacionais do NIST 800 171 13894
Práticas recomendadas operacionais do NIST 800 172 14271
Práticas recomendadas operacionais do NIST 800 181 14351
Práticas recomendadas operacionais do NIST 1800 25 14917
Práticas recomendadas operacionais do NIST CSF 15095
Práticas recomendadas operacionais para o NIST Privacy Framework v1.0 15500
Práticas recomendadas operacionais para o NYDFS 23 15769
Práticas recomendadas operacionais para o CIS 15983
Práticas recomendadas operacionais para o PCI DSS 3.2.1 16070
Práticas recomendadas operacionais para recursos acessíveis ao público 16521
Práticas recomendadas operacionais para a estrutura de segurança cibernética do RBI para UCBs 16522
Práticas recomendadas operacionais para o RBI MD-ITF 16575
Práticas recomendadas operacionais para serviços de segurança, identidade e conformidade 16743
Práticas recomendadas operacionais para tecnologia sem servidor 16743
Práticas recomendadas operacionais para serviços de armazenamento 16743
Práticas recomendadas operacionais para SWIFT CSP 16744
Práticas recomendadas de segurança do Amazon Elastic Container Service (Amazon ECS) 16780
Práticas recomendadas de segurança do Amazon Elastic File System (Amazon EFS) 16781
Práticas recomendadas de segurança do Amazon Elastic Kubernetes Service (Amazon EKS) 16781
Melhores práticas de segurança para a Amazon CloudFront 16781
Melhores práticas de segurança para o Amazon OpenSearch Service 16781
Práticas recomendadas de segurança para o Amazon Redshift 16782
Práticas recomendadas de segurança do Amazon Relational Database Service (Amazon RDS) 16782
Práticas recomendadas de segurança do AWS Auto Scaling 16782
Práticas recomendadas de segurança do AWS CloudTrail 16783
Práticas recomendadas de segurança do AWS CodeBuild 16783
Práticas recomendadas de segurança para o Amazon ECR 16783
Práticas recomendadas de segurança do AWS Lambda 16783
Práticas recomendadas de segurança do AWS Network Firewall 16784

Melhores práticas de segurança para a Amazon SageMaker 16784
Práticas recomendadas de segurança do AWS Secrets Manager 16784
Práticas recomendadas de segurança do AWS WAF 16784
Modelos de exemplo com ação de correção 16785
Pacotes de conformidade personalizados 16785
Terminologia 16785
Personalizar o modelo 16786
Implantar seu pacote de conformidade personalizado 16790
Painel de controle do pacote de conformidade 16790
Navegar pela página principal dos pacotes de conformidade 16791
Saiba mais 16791
Exibir histórico de compatibilidade 16792
Visualizar o cronograma de conformidade 16793
Consultar histórico de conformidade 16793
Implantando um pacote de conformidade (console) 16795
Implante um pacote de conformidade usando modelos 16795
Editar um pacote de conformidade 16797
Excluir um pacote de conformidade 16797
Implantar um pacote de conformidade (AWS CLI) 16798
Implantar um pacote de conformidade 16798
Visualizar um pacote de conformidade 16799
Visualizar o status do pacote de conformidade 16800
Visualizar o status de conformidade do pacote de conformidade 16801
Obter detalhes de conformidade de um pacote de conformidade específico 16801
Excluir um pacote de conformidade 16802
Gerenciar pacotes de conformidade (API) 16803
Gerenciar pacotes de conformidade organizacional 16803
Considerações 16804
Implantação 16805
Suporte regional 16805
Solução de problemas 16808
Status de falha em um pacote de conformidade 16808
Regras pendentes em um pacote de conformidade 16809
Agregadores 16812
Casos de uso 16812
Terminologia 16813

Como agregar dados 16813
Suporte regional 16814
Solução de problemas 16818
Painel do agregador 16820
Usando o Painel do Agregador 16820
Painel de conformidade 16823
Painel de Inventário 16825
Configuração de um agregador (console) 16827
Criar um agregador 16828
Editar um agregador 16830
Excluir um agregador 16830
Configuração de um agregador (AWS CLI) 16831
Adicionar um agregador usando contas individuais 16831
Adicionar um agregador usando o AWS Organizations 16833
Registrar um administrador delegado 16834
Visualizar um agregador 16836
Editar um agregador 16838
Excluir um agregador 16839
Autorização de contas de agregador (console) 16839
Considerações 16840
Adicionar autorização para contas e regiões do agregador 16840
Autorizar uma solicitação pendente para uma conta do agregador 16841
Exclua uma autorização de uma conta de agregador existente 16841
Autorização de contas de agregador (AWS CLI) 16842
Considerações 16842
Adicionar autorização para contas e regiões do agregador 16843
Excluir uma conta de autorização 16843
Consultas avançadas 16845
Atributos 16846
Componentes da consulta 16846
Resumo 16846
Parâmetros 16847
Exemplos 16847
Consultas de exemplo 16847
Exemplos de consultas de relacionamento 16853
Limitações 16855

Suporte regional 16858
Editor de consultas (console) 16862
Considerações 16862
Use uma consulta AWS de amostra 16863
Crie sua consulta personalizada 16863
Editor de consultas (AWS CLI) 16864
Considerações 16865
Dados de configuração do recurso de consulta 16865
Salvar uma consulta 16867
Exibir todas as consultas salvas 16868
Obter detalhes de uma consulta salva 16868
Excluir uma consulta salva 16869
Processador de consultas em linguagem natural 16869
Considerações 16869
Consultar usando o processador de consultas em linguagem natural 16863
Exemplos de solicitações 16871
Fornecer feedback 16874
Suporte regional 16875
Como excluir dados do 16876
Definição do período de retenção de dados (console) 16878
Segurança 16880
Proteção de dados 16881
Criptografia de dados em trânsito 16882
Criptografia de dados em trânsito 16882
Identity and Access Management 16882
Público 16883
Autenticando com identidades 16883
Gerenciando acesso usando políticas 16887
Como AWS Config funciona com o IAM 16890
Exemplos de políticas baseadas em identidade 16898
AWS políticas gerenciadas 16916
Permissões do perfil do IAM 17063
Atualizar o perfil do IAM 17067
Permissões para o Amazon S3 Bucket 17068
Permissões para a chave do KMS 17073
Permissões para o tópico Amazon SNS 17076

Solução de problemas 17080
Uso de perfis vinculadas ao serviço 17082
Resposta a incidentes 17084
Compliance Validation 17084
Resiliência 17086
Segurança da infraestrutura 17086
Análise de configuração e vulnerabilidade 17087
Prevenção contra o ataque do “substituto confuso” em todos os serviços 17087
Práticas recomendadas 17088
Registro e Monitoramento 17089
Registro em log 17089
AWS Config Informações em CloudTrail 17089
Compreendendo as entradas do arquivo de AWS Config log 17090
Exemplos de arquivos de registros 17091
Monitorar 17099
Como usar o Amazon SQS 17099
Usando a Amazon EventBridge 17101
Endpoints da Amazon VPC 17107
Crie um VPC Endpoint para AWS Config 17107
Perguntas frequentes 17108
Não consigo ver minhas últimas alterações de configuração 17108
Posso esperar ver minhas alterações de configuração imediatamente? 17108
Relações indiretas em AWS Config 17108
O que é relacionamento de recursos? 17108
O que é uma relação direta e indireta referente a um recurso? 17109
Quais relacionamentos indiretos AWS Config apoiam? 17109
Como os itens de configuração são criados devido ao relacionamento direto e indireto? . 17111
Quais são os itens de configuração gerados devido a relacionamentos indiretos? 17111
Como faço para recuperar dados de configuração relacionados a relacionamentos indiretos? 17113
Exemplos de código 17115
Ações 17115
`DeleteConfigRule` 17116
`DescribeComplianceByConfigRule` 17118
`DescribeComplianceByResource` 17120
`DescribeConfigRuleEvaluationStatus` 17122

`DescribeConfigRules` 17124
`DescribeConfigurationRecorderStatus` 17127
`DescribeConfigurationRecorders` 17128
`DescribeDeliveryChannels` 17130
`GetComplianceDetailsByConfigRule` 17131
`GetComplianceDetailsByResource` 17134
`GetComplianceSummaryByConfigRule` 17135
`GetComplianceSummaryByResourceType` 17137
`PutConfigRule` 17139
`PutDeliveryChannel` 17143
Histórico do documento 17146
Atualizações anteriores 17262
..... 17334

O que é AWS Config?

AWS Config fornece uma visão detalhada da configuração dos AWS recursos em sua AWS conta. Isso inclui como os recursos estão relacionados um com o outro e como eles foram configurados no passado, de modo que você possa ver como os relacionamentos e as configurações foram alterados ao longo do tempo.

Um AWS recurso é uma entidade com a qual você pode trabalhar AWS, como uma instância do Amazon Elastic Compute Cloud (EC2), um volume do Amazon Elastic Block Store (EBS), um grupo de segurança ou uma Amazon Virtual Private Cloud (VPC). Para obter uma lista completa dos AWS recursos suportados pelo AWS Config, consulteTipos de recursos compatíveis.

Considerações

- Conta da AWS: Você precisa de um ativo Conta da AWS. Para obter mais informações, consulte Inscrever-se em AWS.
- Amazon S3 Bucket: você precisa de um bucket S3 para receber dados para seus snapshots e histórico de configuração. Para obter mais informações, consulte Permissões para buckets do Amazon S3.
- Tópico do Amazon SNS: Você precisa de um Amazon SNS para receber notificações quando houver alterações em seus snapshots e histórico de configuração. Para obter mais informações, consulte Permissões para o tópico do Amazon SNS.
- Função do IAM: você precisa de uma função do IAM que tenha as permissões necessárias para acessar AWS Config. Para obter mais informações, consulte Permissões para a função do IAM.
- Tipos de recursos: você pode decidir quais tipos de recursos AWS Config deseja registrar. Para obter mais informações, consulte AWS Recursos de gravação.

Maneiras de usar AWS Config

Quando você executa seus aplicativos AWS, geralmente usa AWS recursos, que devem ser criados e gerenciados coletivamente. À medida que a demanda por seu aplicativo continua crescendo, também aumenta sua necessidade de controlar seus AWS recursos. AWS Config foi projetado para ajudar você a supervisionar os recursos do seu aplicativo nos seguintes cenários:

Administração de recursos

Para ter melhor governança sobre as configurações de recursos e para detectar erros de configuração, você precisa de visibilidade minuciosa, a qualquer momento, sobre os recursos existentes e como eles estão configurados. Você pode usá-lo AWS Config para notificá-lo sempre que recursos forem criados, modificados ou excluídos sem precisar monitorar essas alterações pesquisando as chamadas feitas para cada recurso.

Você pode usar AWS Config regras para avaliar as configurações dos seus AWS recursos. Quando AWS Config detecta que um recurso viola as condições em uma de suas regras, AWS Config sinaliza o recurso como não compatível e envia uma notificação. AWS Config avalia continuamente seus recursos à medida que são criados, alterados ou excluídos.

Auditoria e Compatibilidade

Você pode estar trabalhando com dados que exijam auditorias frequentes para garantir a compatibilidade com políticas internas e práticas recomendadas. Para demonstrar compatibilidade, você precisa acessar o histórico de configurações de seus recursos. Essas informações são fornecidas por AWS Config.

Gerenciar e solucionar problemas de alteração de configuração

Quando você usa vários AWS recursos que dependem uns dos outros, uma alteração na configuração de um recurso pode ter consequências inesperadas nos recursos relacionados. Com AWS Config, você pode ver como o recurso que você pretende modificar está relacionado a outros recursos e avaliar o impacto de sua alteração.

Você também pode usar o histórico de configurações de seus recursos, fornecido pelo AWS Config , para solucionar problemas e para acessar a última configuração válida de um recurso com problema.

Análise de segurança

Para analisar possíveis pontos fracos de segurança, você precisa de informações históricas detalhadas sobre suas configurações de AWS recursos, como as permissões AWS Identity and Access Management (IAM) concedidas aos seus usuários ou as regras do grupo de segurança do Amazon EC2 que controlam o acesso aos seus recursos.

Você pode usar AWS Config para visualizar a política do IAM que foi atribuída a um usuário, grupo ou função a qualquer momento em que AWS Config estava gravando. Essas informações podem

ajudar você a saber quais as permissões que pertenciam a um usuário em um momento específico: por exemplo, você pode visualizar se o usuário `John Doe` tinha permissão para modificar as configurações da Amazon VPC em 1º de janeiro de 2015.

Você também pode usar AWS Config para visualizar a configuração de seus grupos de segurança do EC2, incluindo as regras de porta que foram abertas em um horário específico. Essas informações podem ajudar você a saber se um grupo de segurança bloqueou tráfego TCP de entrada para uma porta específica.

Soluções para parceiros

AWS faz parceria com especialistas terceirizados em registro e análise para fornecer soluções que usam AWS Config resultados. Para obter mais informações, visite a página de AWS Config detalhes em AWS Config.

Atributos

Ao configurar AWS Config, você pode concluir o seguinte:

Gerenciamento de recursos

- Especifique os tipos de recursos que você AWS Config deseja registrar.

- Configure um bucket do Amazon S3 para receber um snapshot de configuração mediante solicitação e o histórico de configuração.
- Configure o Amazon SNS para enviar notificações do fluxo de configurações.
- AWS Config Conceda as permissões necessárias para acessar o bucket do Amazon S3 e o tópico do Amazon SNS.

  Para obter mais informações, consulte Exibindo configurações e histórico de AWS recursos e Gerenciando configurações e histórico de AWS recursos.

Pacotes de regras e conformidade

- Especifique as regras que você deseja usar AWS Config para avaliar as informações de conformidade dos tipos de recursos registrados.
- Use pacotes de conformidade ou uma coleção de AWS Config regras e ações de remediação que podem ser implantadas e monitoradas como uma única entidade em seu. Conta da AWS

Para obter mais informações, consulte Avaliação de recursos com pacotes de AWS Config regras e conformidade.

Agregadores

- Use um agregador para obter uma visão centralizada do inventário e da conformidade dos recursos. Um agregador coleta dados AWS Config de configuração e conformidade de várias Contas da AWS AWS regiões em uma única conta e região.

  Para obter mais informações, consulte Agregação de dados de várias contas e regiões.

Consultas avançadas

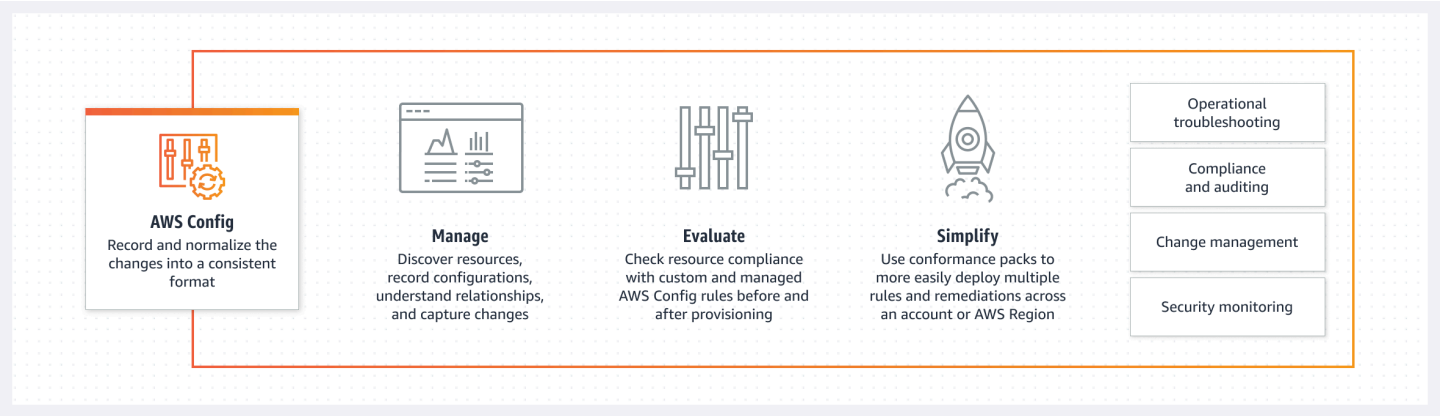
- Use uma das consultas de amostra ou escreva sua própria consulta consultando o esquema de configuração do AWS recurso.

  Para obter mais informações, consulte Consultando o estado atual da configuração dos AWS recursos.

Como AWS Config funciona

AWS Config fornece uma visão detalhada da configuração dos AWS recursos em sua AWS conta. Isso inclui como os recursos estão relacionados um com o outro e como eles foram configurados no passado, de modo que você possa ver como os relacionamentos e as configurações foram alterados ao longo do tempo.

Um AWS recurso é uma entidade com a qual você pode trabalhar AWS, como uma instância do Amazon Elastic Compute Cloud (EC2), um volume do Amazon Elastic Block Store (EBS), um grupo de segurança ou uma Amazon Virtual Private Cloud (VPC). Para obter uma lista completa dos AWS recursos suportados pelo AWS Config, consulteTipos de recursos compatíveis.



Descoberta de recursos

Quando você ativa AWS Config, ele primeiro descobre os AWS recursos compatíveis que existem na sua conta e gera um item de configuração para cada recurso.

AWS Config também gera itens de configuração quando a configuração de um recurso é alterada e mantém registros históricos dos itens de configuração de seus recursos a partir do momento em que você inicia o gravador de configuração. Por padrão, AWS Config cria itens de configuração para cada recurso suportado na região. Se você não quiser AWS Config criar itens de configuração para todos os recursos compatíveis, você pode especificar os tipos de recursos que você deseja monitorar.

Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você está AWS Config configurando. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja compatível com a AWS região em que você está configurando AWS Config.

Acompanhamento de recursos

AWS Config acompanha todas as alterações em seus recursos invocando a chamada da API Describe ou List para cada recurso em sua conta. O serviço usa essas mesmas chamadas de API para capturar detalhes de configuração para todos os recursos relacionados.

Por exemplo, remover uma regra de saída de um grupo de segurança da VPC AWS Config faz com que uma chamada da API Descreve seja invocada no grupo de segurança. AWS Config em seguida, invoca uma chamada da API Describe em todas as instâncias associadas ao grupo de segurança. As configurações atualizadas do grupo de segurança (o recurso) e de cada instância (os recursos

relacionados) são registradas como itens de configuração e entregues em um fluxo de configuração para um bucket do Amazon Simple Storage Service (Amazon S3).

AWS Config também rastreia as alterações de configuração que não foram iniciadas pela API. AWS Config examina as configurações dos recursos periodicamente e gera itens de configuração para as configurações que foram alteradas.

Se você estiver usando AWS Config regras, avalia AWS Config continuamente suas configurações de AWS recursos para as configurações desejadas. Dependendo da regra, AWS Config avaliará seus recursos em resposta às alterações de configuração ou periodicamente. Cada regra é associada a uma função AWS Lambda , que contém a lógica de avaliação para a regra. Quando AWS Config avalia seus recursos, ele invoca a função da regra. AWS Lambda A função retorna o status de compatibilidade dos recursos avaliados. Se um recurso violar as condições de uma regra, AWS Config sinaliza o recurso e a regra como não compatíveis. Quando o status de conformidade de um recurso muda, AWS Config envia uma notificação para seu tópico do Amazon SNS.

Entrega de itens de configuração

AWS Config pode fornecer itens de configuração por meio de um dos seguintes canais:

Bucket do Amazon S3

AWS Config rastreia alterações na configuração de seus AWS recursos e envia regularmente detalhes de configuração atualizados para um bucket do Amazon S3 que você especificar. Para cada tipo de recurso que AWS Config registra, ele envia um arquivo de histórico de configuração a cada seis horas. Cada arquivo de histórico de configuração contém detalhes sobre os recursos alterados naquele período de seis horas. Cada arquivo inclui recursos de um tipo, como instâncias do Amazon EC2 ou volumes do Amazon EBS. Se nenhuma alteração na configuração ocorrer, AWS Config não envia um arquivo.

AWS Config envia um snapshot de configuração para seu bucket do Amazon S3 quando você usa o comando deliver-config-snapshot com a CLI ou quando usa AWS a ação Snapshot com a API. DeliverConfig AWS Config Um instantâneo de configuração contém detalhes de configuração de todos os recursos que são AWS Config registrados em seu Conta da AWS. O arquivo de histórico de configuração e o snapshot de configuração estão no formato JSON.

> **Note**
>
> AWS Config entrega somente os arquivos de histórico de configuração e os instantâneos de configuração para o bucket do S3 especificado; AWS Config não modifica as políticas

de ciclo de vida dos objetos no bucket do S3. Você pode usar políticas de ciclo de vida para especificar se deseja excluir ou arquivar objetos para o Amazon S3 Glacier. Para obter mais informações, consulte Managing Lifecycle Configuration no Guia do usuário do Amazon Simple Storage Service. Você também pode ver a publicação Archiving &S3; Data to &GL;, no blog.

Tópico do Amazon SNS

Um tópico do Amazon Simple Notification Service (Amazon SNS) é um canal de comunicação usado pelo Amazon SNS para entregar mensagens (ou notificações) a endpoints inscritos, como um endereço de e-mail ou clientes. Outros tipos de notificações do Amazon SNS incluem as mensagens de notificação por push para aplicações em telefones celulares, notificações de SMS (Short Message Service) para celulares e smartphones habilitados por SMS e solicitações HTTP POST. Para obter melhores resultados, use o Amazon SQS como o endpoint da notificação para o tópico SNS e, em seguida, processe as informações da notificação de forma programática.

AWS Config usa o tópico do Amazon SNS que você especifica para enviar notificações. O tipo de notificação que você está recebendo é indicado pelo valor para a chave `messageType` no corpo da mensagem, como no exemplo a seguir:

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

As notificações podem ser de qualquer um dos seguintes tipos de mensagem.

Tipo de mensagem	Descrição
ComplianceChangeNotificação	O tipo de conformidade de um recurso que AWS Config avalia mudou. O tipo de conformidade indica se o recurso está em conformidade com uma AWS Config regra específica e é representado pela `ComplianceType` chave na mensagem. A mensagem inclui os objetos `newEvaluationResult` e `oldEvaluationResult` para comparação.
ConfigRulesEvaluationStarted	AWS Config começou a avaliar sua regra em relação aos recursos especificados.

Tipo de mensagem	Descrição
ConfigurationSnapshotDeliveryStarted	AWS Config começou a entregar o snapshot de configuração para seu bucket do Amazon S3. O nome do bucket do Amazon S3 é fornecido para a chave `s3Bucket` na mensagem.
ConfigurationSnapshotDeliveryCompleted	AWS Config entregou com sucesso o snapshot de configuração para seu bucket do Amazon S3.
ConfigurationSnapshotDeliveryFailed	AWS Config falha ao entregar o snapshot de configuração para seu bucket do Amazon S3.
ConfigurationHistoryDeliveryCompleted	AWS Config entregou com sucesso o histórico de configuração para seu bucket do Amazon S3.
ConfigurationItemChangeNotification	Um recurso foi criado, excluído ou alterado na configuração. Essa mensagem inclui os detalhes do item de configuração AWS Config criado para essa alteração e inclui o tipo de alteração. Essas notificações são entregues minutos após uma alteração e são coletivam ente conhecidas como stream de configuração.
OversizedConfigurationItemChangeNotification	Esse tipo de mensagem é entregue quando uma notificação de alteração de item de configuração excedeu o tamanho máximo permitido pelo Amazon SNS. A mensagem inclui um resumo do item de configuração. Com exceção das mensagens SMS, as mensagens do Amazon SNS podem conter até 256 KB de dados de texto, incluindo XML, JSON e texto não formatado. Você pode visualizar a notificaç ão completa no local do bucket do Amazon S3 especificado.

Tipo de mensagem	Descrição
OversizedConfigurationItemChangeDeliveryFailed	AWS Config falhou em entregar a notificação de alteração de item de configuração de tamanho grande para seu bucket do Amazon S3.

Por exemplos de notificação, consulte Notificações que o AWS Config envia para um tópico do Amazon SNS. Para obter mais informações sobre tópicos do Amazon SNS, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

> **Note**
>
> Por que não consigo ver minhas últimas alterações de configuração?
> AWS Config geralmente registra as alterações de configuração em seus recursos logo após a detecção de uma alteração ou na frequência especificada por você. No entanto, isso é feito com base no melhor esforço e às vezes pode levar mais tempo. Se os problemas persistirem depois de algum tempo, entre em contato AWS Supporte forneça suas AWS Config métricas que são suportadas pela Amazon. CloudWatch Para obter informações sobre essas métricas, consulte Métricas de AWS Config uso e sucesso.

Controle o acesso ao AWS Config

AWS Identity and Access Management é um serviço web que permite que os clientes da Amazon Web Services (AWS) gerenciem usuários e permissões de usuários.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:

- Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Conceitos

AWS Config fornece uma visão detalhada dos recursos associados aos seus Conta da AWS, incluindo como eles são configurados, como estão relacionados entre si e como as configurações e seus relacionamentos mudaram ao longo do tempo. Vamos analisar os conceitos do AWS Config.

Sumário

- AWS Config Interfaces
  - AWS Config Console
  - AWS Config CLI
  - AWS Config APIs
  - AWS Config SDKs
- Gerenciamento de recursos
  - AWS Recursos
  - Relacionamento de recursos
- Gravador de configuração
- Nome do canal de entrega
  - Itens de configuração
  - Histórico de configuração
  - Snapshot de configuração
  - Stream de configuração
- AWS Config Regras
  - AWS Config Regras gerenciadas
  - AWS Config Regras personalizadas
  - Tipos de trigger
  - Modos de avaliação

- Pacotes de conformidade
- Agregação de dados de várias regiões e várias contas
  - Conta de origem
  - Região de origem
  - Agregador
  - Conta de agregador
  - Autorização

AWS Config Interfaces

AWS Config Console

Você pode gerenciar o serviço usando o AWS Config console. Para obter mais informações sobre o AWS Management Console, consulte AWS Management Console.

AWS Config CLI

AWS Command Line Interface É uma ferramenta unificada que você pode usar para interagir na linha AWS Config de comando. Para obter mais informações, consulte o AWS Command Line Interface Guia de usuário do . Para obter uma lista completa dos comandos da AWS Config CLI, consulte Comandos disponíveis.

AWS Config APIs

Além do console e da CLI, você também pode usar as APIs AWS Config RESTful para programar diretamente. AWS Config Para obter mais informações, consulte a AWS Config Referência da API do .

AWS Config SDKs

Como alternativa ao uso da AWS Config API, você pode usar um dos AWS SDKs. Cada SDK consiste em bibliotecas e código de exemplo para várias plataformas e linguagens de programação. Os SDKs são uma forma conveniente de criar acesso programático ao AWS Config. Por exemplo, você pode usar os SDKs para assinar solicitações de maneira criptográfica, gerenciar erros e realizar automaticamente novas tentativas de solicitações. Para obter mais informações, consulte a página Ferramentas para o Amazon Web Services.

Gerenciamento de recursos

Compreender os componentes básicos do AWS Config ajudará você a monitorar o inventário e as alterações de recursos e avaliar as configurações de seus AWS recursos.

AWS Recursos

AWS recursos são entidades que você cria e gerencia usando o AWS Management Console, a AWS Command Line Interface (CLI), os AWS SDKs ou AWS as ferramentas de parceiros. Exemplos de AWS recursos incluem instâncias do Amazon EC2, grupos de segurança, Amazon VPCs e Amazon Elastic Block Store. AWS Config refere-se a cada recurso usando seu identificador exclusivo, como o ID do recurso ou um nome de recurso da Amazon (ARN). Para obter uma lista dos tipos de recursos AWS Config compatíveis, consulteTipos de recursos compatíveis.

Relacionamento de recursos

AWS Config descobre AWS recursos em sua conta e, em seguida, cria um mapa das relações entre os AWS recursos. Por exemplo, um relacionamento pode incluir um volume `vol-123ab45d` do Amazon EBS anexado a uma instância `i-a1b2c3d4` do Amazon EC2, que esteja associada ao grupo de segurança `sg-ef678hk`.

Para ter mais informações, consulte Tipos de recursos compatíveis.

Gravador de configuração

O gravador de configuração armazena as configurações dos recursos compatíveis na conta como itens de configuração. Você deve primeiro criar e, em seguida, iniciar o gravador de configuração antes de começar a gravação. Você pode interromper e reiniciar o gravador de configuração a qualquer momento. Para ter mais informações, consulte Gerenciar o gravador de configurações.

Por padrão, o gravador de configuração registra todos os recursos suportados na região em que AWS Config está sendo executado. Você pode criar um gravador de configuração personalizado que registra apenas os tipos de recursos que você especificar. Para ter mais informações, consulte AWS Recursos de gravação.

Se você usa a CLI AWS Management Console ou a CLI para ativar o serviço, cria e inicia AWS Config automaticamente um gravador de configuração para você.

Nome do canal de entrega

Ao registrar AWS Config continuamente as alterações que ocorrem em seus AWS recursos, ele envia notificações e estados de configuração atualizados por meio do canal de entrega. Você pode gerenciar o canal de entrega para controlar para onde AWS Config envia as atualizações de configuração.

Itens de configuração

Um item de configuração representa uma point-in-time visualização dos vários atributos de um AWS recurso compatível que existe em sua conta. Os componentes de um item de configuração incluem metadados, atributos, relacionamentos, configuração atual e eventos relacionados. AWS Config cria um item de configuração sempre que detecta uma alteração em um tipo de recurso que está gravando. Por exemplo, se AWS Config estiver gravando buckets do Amazon S3, AWS Config cria um item de configuração sempre que um bucket é criado, atualizado ou excluído. Você também pode selecionar AWS Config para criar um item de configuração na frequência de gravação definida.

Para obter mais informações, consulte Components of a Configuration Item e Selecting Which Resources are Recorded | Recording Frequency.

Histórico de configuração

Histórico de configuração é uma coleção de itens de configuração para um recurso específico durante um período. Um histórico de configuração pode ajudar a responder perguntas sobre, por exemplo, quando o recurso foi criado, como o recurso foi configurado no decorrer do último mês, e que alterações de configuração foram feitas ontem, às 9h. O histórico de configuração está disponível para você em vários formatos. AWS Config entrega automaticamente um arquivo de histórico de configuração para cada tipo de recurso que está sendo gravado em um bucket do Amazon S3 que você especificar. Você pode selecionar um determinado recurso no AWS Config console e navegar até todos os itens de configuração anteriores desse recurso usando a linha do tempo. Além disso, você pode acessar o histórico de itens de configuração para um recurso a partir da API.

Para obter mais informações, consulte Exibindo configurações e histórico de AWS recursos e Gerenciando configurações e histórico de AWS recursos.

Snapshot de configuração

Snapshot de configuração é uma coleção de itens de configuração dos recursos compatíveis existentes na conta. Esse snapshot de configuração é uma imagem completa dos recursos que estão

sendo registrados e suas configurações. O snapshot de configuração pode ser uma ferramenta útil para validar sua configuração. Por exemplo, talvez você queira examinar o snapshot de configuração regularmente para recursos que são configurados incorretamente ou que potencialmente não devem existir. O snapshot de configuração está disponível em vários formatos. O snapshot de configuração pode ser enviado a um bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Além disso, você pode selecionar um momento no AWS Config console e navegar pelo instantâneo dos itens de configuração usando as relações entre os recursos.

Stream de configuração

Um fluxo de configuração é uma lista atualizada automaticamente de todos os itens de configuração dos recursos que estão AWS Config sendo gravados. Toda vez que um recurso é criado, modificados ou excluídos, o AWS Config cria um item de configuração e o adiciona ao stream de configuração. O fluxo de configuração funciona usando um tópico do Amazon Simple Notification Service (Amazon SNS) de sua escolha. O fluxo de configuração é útil para observar as alterações de configuração à medida que elas ocorrem, para que você possa identificar possíveis problemas, gerar notificações se determinados recursos forem alterados ou atualizar sistemas externos que precisam refletir a configuração de seus AWS recursos.

AWS Config Regras

Uma AWS Config regra representa as configurações desejadas para AWS recursos específicos ou para um todo Conta da AWS. Se um recurso não passar por uma verificação de regras, AWS Config sinaliza o recurso e a regra como não compatíveis e AWS Config notifica você por meio do Amazon SNS. A seguir estão os possíveis resultados da avaliação de uma AWS Config regra:

- `COMPLIANT`: a regra passa pelas condições da verificação de conformidade.
- `NON_COMPLIANT`: a regra não cumpre as condições da verificação de conformidade.
- `ERROR`: um dos parâmetros obrigatórios/opcionais não é válido, não é do tipo correto ou está formatado incorretamente.
- `NOT_APPLICABLE`: usado para filtrar recursos aos quais a lógica da regra não pode ser aplicada. Por exemplo, a regra alb-desync-mode-check verifica somente os Application Load Balancers e ignora os Network Load Balancers e os Gateway Load Balancers.

Há dois tipos de regras: regras AWS Config gerenciadas e regras AWS Config personalizadas. Para obter mais informações sobre a estrutura de definições de regras e metadados de regras, consulte Componentes de uma AWS Config regra.

AWS Config Regras gerenciadas

AWS Config As regras gerenciadas são regras predefinidas e personalizáveis criadas por. AWS Config Para obter uma lista de regras gerenciadas, consulte Lista de regras AWS Config gerenciadas.

AWS Config Regras personalizadas

AWS Config Regras personalizadas são regras que você cria do zero. Há duas maneiras de criar regras AWS Config personalizadas: com as funções Lambda (Guia do AWS Lambda desenvolvedor) e com o Guard (Guard GitHub Repository), uma linguagem. policy-as-code AWS Config as regras personalizadas criadas com AWS Lambda são chamadas de Regras Lambda AWS Config Personalizadas e as regras AWS Config personalizadas criadas com o Guard são chamadas de Regras de Política AWS Config Personalizadas.

Para ver um passo a passo mostrando como criar regras de política AWS Config personalizadas, consulte Criação de regras de política AWS Config personalizadas. Para ver um passo a passo mostrando como criar regras personalizadas do AWS Config Lambda, consulte Criação de regras personalizadas AWS Config do Lambda.

Tipos de trigger

Depois de adicionar uma regra à sua conta, AWS Config compara seus recursos com as condições da regra. Após essa avaliação inicial, AWS Config continua executando avaliações cada vez que uma é acionada. Os gatilhos de avaliação são definidos como parte da regra e podem incluir os seguintes tipos.

Tipo de gatilho	Descrição
Alterações de configuração	AWS Config executa avaliações para a regra quando há um recurso que correspon de ao escopo da regra e há uma alteração na configuração do recurso. A avaliação é executada após o AWS Config envio de uma notificação de alteração do item de configura ção.

Tipo de gatilho	Descrição
	Você escolhe quais recursos acionam a avaliação, definindo o escopo da regra. O escopo pode incluir o seguinte: • Um ou mais tipos de recursos • A combinação de um tipo de recurso e um ID de recurso • A combinação de uma chave de tag e valor • Quando os recursos registrados são criados, atualizados ou excluídos AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponde ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações.
Periódico	AWS Config executa avaliações para a regra na frequência que você escolher; por exemplo, a cada 24 horas.
Híbrida	Algumas regras têm alterações na configura ção e gatilhos periódicos. Para essas regras, AWS Config avalia seus recursos ao detectar uma alteração na configuração e também na frequência especificada.

Modos de avaliação

Há dois modos de avaliação das AWS Config regras.

Modo de avaliação	Descrição
Proativo	Use a avaliação proativa para avaliar os recursos antes de serem implantados. Isso

Modo de avaliação	Descrição
	permite avaliar se um conjunto de proprieda des de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região. Para obter mais informações, consulte Modos de avaliação. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.
Detecção	Use a avaliação de detecção para avaliar os recursos que já foram implantados. Isso permite avaliar as definições de configuração de seus recursos existentes.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Pacotes de conformidade

Um pacote de conformidade é um conjunto de AWS Config regras e ações de remediação que podem ser facilmente implantadas como uma única entidade em uma conta e uma região ou em uma organização em. AWS Organizations

Os pacotes de conformidade são criados usando um modelo YAML criado por você que contenha a lista de regras gerenciadas ou personalizadas do AWS Config e as ações de correção. É possível implantar o modelo usando o console do AWS Config ou a AWS CLI.

Para começar rapidamente e avaliar seu AWS ambiente, use um dos exemplos de modelos de pacote de conformidade. Você também pode criar um arquivo YAML do pacote de conformidade

do zero com base no Pacote de conformidade personalizado. Um pacote de conformidade personalizado é uma coleção exclusiva de AWS Config regras e ações de remediação que você pode implantar juntas em uma conta e uma AWS região, ou em uma organização em. AWS Organizations

As verificações de processo são um tipo de AWS Config regra que permite rastrear suas tarefas externas e internas que exigem verificação como parte dos pacotes de conformidade. Essas verificações podem ser adicionadas a um pacote de conformidade existente ou a um novo pacote de conformidade. Você pode monitorar toda a conformidade, incluindo AWS Config prazos e verificações manuais, em um único local.

Agregação de dados de várias regiões e várias contas

A agregação de dados multiconta e multirregional AWS Config permite agregar dados de AWS Config configuração e conformidade de várias contas e regiões em uma única conta. A agregação de dados multirregionais de várias contas é útil para que os administradores centrais de TI monitorem a conformidade de várias Contas da AWS pessoas na empresa. O uso de agregadores não incorre em custos adicionais.

Conta de origem

Uma conta de origem é a Conta da AWS partir da qual você deseja agregar dados de configuração e conformidade de AWS Config recursos. Uma conta de origem pode ser uma conta individual ou uma organização no AWS Organizations. Você pode fornecer contas de origem individualmente ou recuperá-las por meio AWS Organizations de.

Região de origem

Uma região de origem é a AWS região da qual você deseja agregar dados de AWS Config configuração e conformidade.

Agregador

Um agregador coleta dados de AWS Config configuração e conformidade de várias contas e regiões de origem. Crie um agregador na região em que você deseja ver os dados agregados de AWS Config configuração e conformidade.

> **Note**
>
> Os agregadores fornecem uma visão somente para leitura das contas e regiões de origem que o agregador está autorizado a visualizar, replicando dados das contas de origem na conta do agregador. Os agregadores não fornecem acesso mutável a uma conta ou região de origem. Por exemplo, isso significa que você não pode implantar regras por meio de um agregador ou enviar arquivos de instantâneos para uma conta ou região de origem por meio de um agregador.

Conta de agregador

Uma conta de agregador é uma conta na qual você cria um agregador.

Autorização

Como proprietário da conta de origem, a autorização se refere às permissões que você concede a uma conta agregadora e a uma região para coletar seus dados de AWS Config configuração e conformidade. A autorização não é necessária se você estiver agregando contas de origem que fazem parte do AWS Organizations.

Suporte regional

> **Note**
>
> Alguns recursos do AWS Config são compatíveis somente em um subconjunto das AWS regiões em que AWS Config há suporte.
> Gerenciamento de recursos
>
> - Para obter uma lista de quais tipos de AWS recursos são suportados em quais regiões, consulte Cobertura de recursos por disponibilidade regional.
>
> AWS Config Regras
>
> - Para obter uma lista de quais AWS Config regras são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.
> - Para obter uma lista das regiões que oferecem suporte à implantação organizacional de AWS Config regras, consulte Organizational Rules | Region Support.

- Para obter uma lista de regiões que apoiam ações de remediação de AWS Config regras, consulte Remediation Actions | Region Support.

Pacotes de conformidade

- Para obter uma lista de regiões compatível com pacotes de conformidade e a implantação organizacional de pacotes de conformidade, consulte Conformance Packs | Region Support.

Agregadores

- Para obter uma lista das regiões que oferecem suporte aos agregadores, consulte Aggregators | Region Support.

Consultas avançadas

- Para obter uma lista de regiões que oferecem suporte a consultas avançadas, consulte Advanced Queries | Region Support.
- Para obter uma lista de regiões compatíveis com o processador de consulta de linguagem natural para consultas avançadas, consulte Natural language query processor for advanced queries | Region Support.

A tabela a seguir lista as AWS regiões nas quais você pode ativar AWS Config.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS

Nome da região	Região	Endpoint	Protocolo
Oeste dos EUA (Norte da Califórnia)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
África (Cidade do Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milão)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Espanha)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurique)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Service Limits

A tabela a seguir descreve os limites no AWS Config. Salvo indicação em contrário, as cotas podem ser aumentadas mediante solicitação. É possível solicitar um aumento da cota.

Para obter informações sobre outros limites na AWS, consulte Limites do serviço da AWS.

Limites de serviço do AWS Config

Descrição	Valor limite	Pode ser aumentada
Número máximo de regras do AWS Config por região, por conta	1000	Não
Número máximo de tags por recurso	50	Não

Pacotes de conformidade em uma única conta

Descrição	Valor limite	Pode ser aumentada
Número máximo de pacotes de conformidade por conta	50	Não
Número máximo de regras do AWS Config por pacote de conformidade	130	Não

> **Note**
>
> As regras do AWS Config nos pacotes de conformidade são consideradas no limite do número máximo de regras do AWS Config por região, por conta.

Pacotes de conformidade da organização

Descrição	Valor limite	Pode ser aumentada
Número máximo de pacotes de conformidade por organização	50	Não
Número máximo de regras do AWS Config por pacote de conformidade da organização	130	Não

> **Note**
>
> A implantação no nível da organização é considerada no limite de contas filhas. As regras do AWS Config nos pacotes de conformidade são consideradas no limite do número máximo de regras do AWS Config por região, por conta.

Agregadores

Descrição	Valor limite	Pode ser aumentada
Número máximo de agregadores de configuração	50	Sim
Número máximo de contas em um agregador	10000	Não
Número máximo de contas adicionadas ou excluídas por semana para todos os agregadores	1000	Sim

Consultas avançadas

Descrição	Valor limite	Pode ser aumentada
Número máximo de consultas salvas em uma única conta e região	300	Sim

AWS Integrações de serviços com AWS Config

AWS Config suporta integrações com vários outros AWS serviços.

AWS Organizations

Você pode usar AWS Organizations para definir as contas a serem usadas para o recurso de agregação AWS Config de dados multicontas e multirregiões do. AWS Organizations é um serviço de gerenciamento de contas que ajuda você a consolidar várias Contas da AWS em uma organização que você cria e gerencia centralmente. Ao fornecer seus AWS Organizations detalhes, você pode monitorar o status de conformidade em toda a sua organização. Para obter mais informações AWS Config e AWS Organizations no Guia do AWS Organizations usuário.

AWS Control Tower

AWS Control Tower ativa AWS Config em todas as contas inscritas, para que possa monitorar a conformidade por meio de controles de detetive, registrar alterações de recursos e entregar registros de alterações de recursos à conta de arquivamento de registros. Para obter mais informações, consulte Monitorar alterações de recursos AWS Config no Guia AWS Control Tower do usuário.

AWS CloudTrail

AWS Config se integra AWS CloudTrail para correlacionar alterações de configuração a eventos específicos em sua conta. Você pode usar os CloudTrail registros para obter os detalhes do evento que provocou a alteração, incluindo quem fez a solicitação, a que horas e de qual endereço IP. Você pode navegar até a AWS Config linha do tempo a partir do CloudTrail console para ver as alterações de configuração relacionadas às suas atividades de AWS API.

Para obter mais informações, consulte Registrar chamadas de AWS Config API AWS CloudTrail no Guia do AWS Config desenvolvedor e Criar um armazenamento de dados de eventos para itens de AWS Config configuração com o console no Guia AWS CloudTrail do usuário.

AWS Security Hub

AWS Security Hub centraliza as verificações de segurança de outros AWS serviços, incluindo AWS Config regras. O Security Hub habilita e controla AWS Config regras para verificar se suas configurações de recursos estão alinhadas às melhores práticas. Ative AWS Config em todas as contas em todas as regiões em que o Security Hub está executando verificações de segurança nos recursos do seu ambiente. Para obter mais informações, consulte AWS serviços que enviam descobertas para o Security Hub no Guia AWS Security Hub do Usuário.

AWS Audit Manager

Você pode usar o Audit Manager para capturar AWS Config avaliações como evidência para auditorias. Ao criar ou editar um controle personalizado, você pode especificar uma ou mais AWS Config regras como mapeamento da fonte de dados para coleta de evidências. AWS Config executa verificações de conformidade com base nessas regras, e o Audit Manager relata os resultados como evidência de verificação de conformidade. Para obter mais informações, consulte AWS Config Regras suportadas AWS Audit Manager no Guia do AWS Audit Manager usuário.

AWS Systems Manager

AWS Config integra-se ao Systems Manager para registrar alterações de configuração no software em suas instâncias e servidores do Amazon EC2 em seu ambiente local. Com essa integração, você pode obter visibilidade das configurações do sistema operacional (SO), das atualizações no nível do sistema, dos aplicativos instalados, da configuração de rede e muito mais. AWS Config também fornece um histórico das alterações de configuração no sistema operacional e no nível do sistema, juntamente com as alterações na configuração da infraestrutura registradas nas instâncias do Amazon EC2. Você pode navegar até a AWS Config linha do tempo a partir do console do Systems Manager para visualizar as alterações de configuração de suas instâncias gerenciadas do Amazon EC2. Você pode usar AWS Config para visualizar o histórico de inventário do Systems Manager e acompanhar as alterações em todas as suas instâncias gerenciadas.

Para obter mais informações, consulte Integração com AWS serviços | Gerenciamento e governança, gravador de AWS Config configuração e implantação de pacotes de AWS Config conformidade no Guia do AWS Systems Manager usuário.

AWS Firewall Manager

Para usar o Firewall Manager, você deve habilitar AWS Config para cada uma das suas contas de AWS Organizations membros. Quando novos aplicativos são criados, o Firewall Manager é o único serviço para criar regras de firewall, criar políticas de segurança e aplicá-las de forma consistente. Para obter mais informações, consulte Habilitar AWS Config no AWS WAF AWS Firewall Manager, e no Guia AWS Shield Advanced do desenvolvedor.

> **Note**
>
> O Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua. Para obter mais informações sobre gravação contínua e gravação diária, consulte Frequência de gravação.

Hosts dedicados do Amazon EC2

AWS Config integra-se aos hosts dedicados do Amazon EC2 para avaliar a conformidade da licença. AWS Config registra quando as instâncias são iniciadas, interrompidas ou encerradas em um host dedicado e combina essas informações com informações em nível de host e instância relevantes

para o licenciamento de software, como ID de host, IDs de imagem de máquina da Amazon (AMI), número de soquetes e núcleos físicos. Isso ajuda você a usar AWS Config como fonte de dados para seus relatórios de licenças. Você pode navegar até a AWS Config linha do tempo no console de hosts dedicados do Amazon EC2 para ver as alterações de configuração dos seus hosts dedicados do Amazon EC2.

Para obter mais informações, consulte Rastrear alterações de configuração no Guia do usuário do Amazon Elastic Compute Cloud para instâncias Linux ou Rastrear alterações de configuração no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows.

Application Load Balancers

AWS Config integra-se ao serviço Elastic Load Balancing (ELB) para registrar alterações de configuração nos Application Load Balancers. AWS Config também inclui relacionamentos com grupos de segurança, VPCs e sub-redes associados do Amazon EC2. Você pode usar essas informações para análise de segurança e solução de problemas. Por exemplo, você pode verificar quais grupos de segurança estão associados ao seu Application Load Balancer a qualquer momento. Você pode navegar até a AWS Config linha do tempo no console do ELB para ver as alterações de configuração dos seus Application Load Balancers.

AWS CodeBuild

AWS Config fornece um inventário de seus AWS recursos e um histórico das alterações de configuração desses recursos. AWS Config suporta AWS CodeBuild; como um AWS recurso, o que significa que o serviço pode rastrear seus CodeBuild projetos. Para obter mais informações, consulte Usar AWS Config com CodeBuild amostra no Guia AWS CodeBuild do usuário.

AWS X-Ray

AWS X-Ray se integra AWS Config para registrar as alterações de configuração feitas em seus recursos de criptografia do X-Ray. Você pode usar AWS Config para inventariar os recursos de criptografia do X-Ray, auditar o histórico de configuração do X-Ray e enviar notificações com base nas alterações dos recursos. Para obter mais informações, consulte Tracking X-Ray Encryption Changes with AWS Config the AWS X-Ray Developer Guide.

AWS Service Management Connector

O AWS Service Management Connector formulário ServiceNow pode sincronizar AWS Config dados de várias contas e regiões usando um agregador. Para obter mais informações, consulte Integração AWS Config ServiceNow no Guia do AWS Service Management Connector Administrador.

Amazon API Gateway

Você pode usar AWS Config para registrar as alterações de configuração feitas nos recursos da API do API Gateway e enviar notificações com base nas alterações dos recursos. A manutenção de um histórico de alteração de configurações do API Gateway é útil para casos de uso de solução de problemas operacionais, auditoria e conformidade. Para obter mais informações, consulte Monitorando a configuração da API Gateway AWS Config no Guia do desenvolvedor do API Gateway.

Informações complementares e recursos relacionados

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

- AWS Config— A página principal da web para obter informações sobre AWS Config.
- Definição de preço do AWS Config
- Perguntas técnicas frequentes sobre o https://aws.amazon.com/config/faq/
- AWS Config Kit de desenvolvimento de regras (RDK) — Uma ferramenta de código aberto que ajuda você a configurar AWS Config, criar regras e depois testá-las usando uma variedade de tipos de AWS recursos.
- Parceiros — links para produtos de parceiros totalmente integrados AWS Config para ajudá-lo a visualizar, monitorar e gerenciar os dados de seu fluxo de configuração, instantâneos de configuração ou histórico de configuração.
- Aulas e workshops — Links para cursos especializados e baseados em funções, além de laboratórios individualizados para ajudar a aprimorar suas AWS habilidades e ganhar experiência prática.
- AWS Centro do desenvolvedor — explore tutoriais, baixe ferramentas e saiba mais sobre eventos para AWS desenvolvedores.

- AWS Ferramentas para desenvolvedores — Links para ferramentas de desenvolvedor, SDKs, kits de ferramentas de IDE e ferramentas de linha de comando para desenvolver e gerenciar AWS aplicativos.
- Centro de recursos de introdução — Saiba como configurar seu aplicativo Conta da AWS, participar da AWS comunidade e lançar seu primeiro aplicativo.
- Tutoriais práticos — Siga os tutoriais para iniciar seu step-by-step primeiro aplicativo no. AWS
- AWS Whitepapers — Links para uma lista abrangente de AWS white papers técnicos, abrangendo tópicos como arquitetura, segurança e economia e criados por arquitetos de AWS soluções ou outros especialistas técnicos.
- AWS Support Center — O hub para criar e gerenciar seus AWS Support casos. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e. AWS Trusted Advisor
- AWS Support— A principal página da web com informações sobre AWS Support um one-on-one canal de suporte de resposta rápida para ajudá-lo a criar e executar aplicativos na nuvem.
- Entrar em contato:Um ponto central de contato para consultas relativas a faturas da AWS , contas, eventos, uso abusivo e outros problemas.
- AWS Termos do site — Informações detalhadas sobre nossos direitos autorais e nossa marca registrada; sua conta, licença e acesso ao site; e outros tópicos.

AWS Kits de desenvolvimento de software para AWS Config

Um kit AWS de desenvolvimento de software (SDK) facilita a criação de aplicativos que acessam serviços de infraestrutura econômicos, escaláveis e confiáveis AWS . Com os SDKs da AWS , você pode começar a desenvolver em minutos com um único pacote para download, que inclui a biblioteca, exemplos de código e documentação de referência. A tabela a seguir lista os SDKs e as bibliotecas de terceiros disponíveis que você pode usar para acessar AWS Config programaticamente.

Tipo de acesso	Descrição
AWS SDKs	AWS fornece os seguintes SDKs: • AWS Documentação do SDK for C++ • AWS Mobile SDK for iOS Documentação • Documentação do SDK da AWS para Go

Tipo de acesso	Descrição
	• AWS SDK for Java Documentação • AWS SDK para documentação JavaScript • AWS SDK for .NET Documentação • AWS SDK for PHP Documentação • AWS SDK for Python (Boto) Documentação • AWS SDK for Ruby Documentação
Bibliotecas de terceiros	Os desenvolvedores da comunidade de AWS desenvolvedores também fornecem suas próprias bibliotecas, que você pode encontrar nos seguintes centros de AWS desenvolvedores: • AWS Centro do desenvolvedor Java • Centro do desenvolvedor da AWS JavaScript • AWS Centro do desenvolvedor para PHP • AWS Centro de desenvolvedores Python • AWS Centro do desenvolvedor Ruby • AWS Centro de desenvolvedores do Windows e.NET

Começando com AWS Config

AWS Config fornece uma visão detalhada da configuração dos AWS recursos em seu Conta da AWS. Com AWS Config, você pode revisar as alterações nas configurações e nos relacionamentos entre os AWS recursos, explorar o histórico de configuração dos recursos e usar regras para determinar a conformidade. Para obter mais informações, consulte O que é AWS Config? e como AWS Config funciona.

Inscrevendo-se para AWS

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use o URL de login que foi enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Maneiras de começar com AWS Config

Depois de se inscrever em um Conta da AWS, você pode começar a usar AWS Config a AWS Management Console AWS CLI ou os AWS SDKs.

- Configurando AWS Config com o console
- Configurando AWS Config com o AWS CLI
- Usando o AWS Config serviço com o AWS SDK

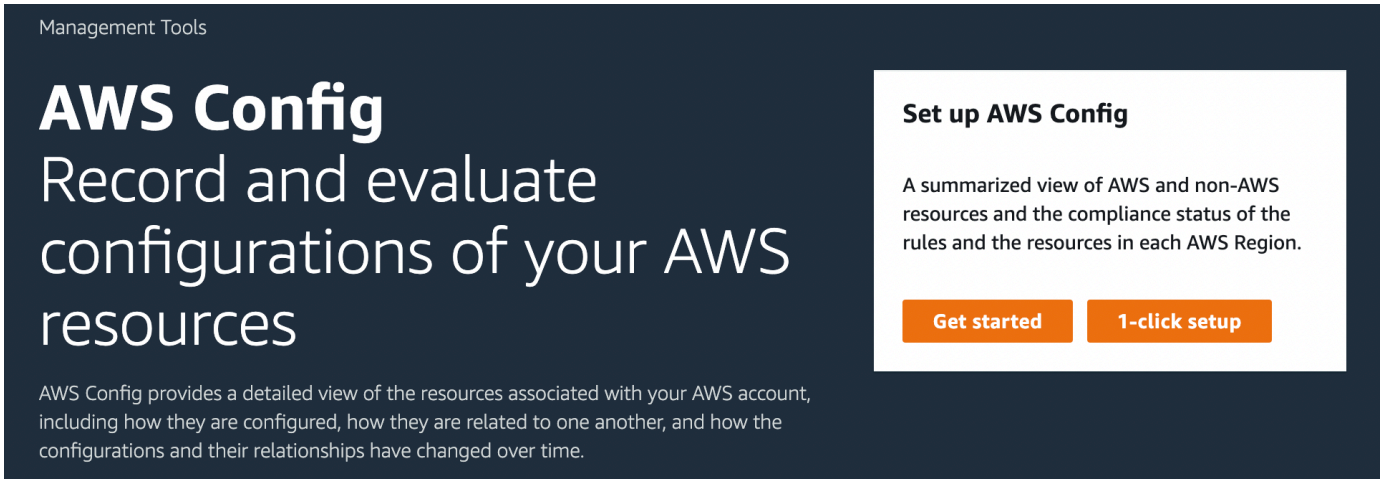
Configurando AWS Config com o console

Isso AWS Management Console fornece um processo rápido e simplificado de configuração. AWS Config

Configuração

Para configurar AWS Config com o console

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Se for a primeira vez que você abre o AWS Config console ou se configura AWS Config em uma nova região, a página do AWS Config console tem a seguinte aparência:



3. Escolha a configuração de 1 clique para iniciar AWS Config com base nas AWS melhores práticas. Você também pode clicar em Comece a usar para um processo de configuração mais detalhado.

Tópicos

- Configuração com um clique
- Configuração manual

Configuração com um clique

AWS Config A configuração com 1 clique ajuda a simplificar o processo inicial para clientes de AWS Config console, reduzindo o número de seleções manuais. Para passar por todas as seleções manuais do processo de configuração, consulte Configuração manual.

Para configurar AWS Config com o console usando a configuração com 1 clique

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configuração com um clique.

A página de configuração inclui três etapas. No entanto, o fluxo de trabalho da opção Configuração com um clique leva você automaticamente à Etapa 3 (Análise). As informações abaixo fornecem um detalhamento desse processo.

- Configurações: Para selecionar a maneira pela qual o AWS Config console registra recursos e funções e escolher para onde o histórico de configuração e os arquivos instantâneos de configuração são enviados.
- Regras: para regiões que oferecem suporte a regras, esta subseção está disponível para você configurar as regras AWS gerenciadas iniciais que você pode adicionar à sua conta.

  Após a configuração, AWS Config avaliará seus AWS recursos de acordo com as regras que você escolheu. É possível criar regras adicionais e atualizar as existentes em sua conta após a configuração. Para obter mais informações sobre regras, consulte Gerenciando suas AWS Config regras.
- Revisão: Para verificar os detalhes da configuração.

Configurações

Estratégia de gravação

A opção de registrar Todos os tipos de recursos com substituições personalizáveis foi selecionada para você. AWS Config registrará todos os tipos de recursos suportados atuais e futuros nesta região. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

- Configurações padrão

  A frequência de gravação padrão é definida como Contínua para você. Isso significa que AWS Config registra as alterações de configuração continuamente sempre que uma alteração ocorre.

  AWS Config também suporta a opção de definir a frequência de gravação como Diária. Se você selecionar essa opção após a configuração, receberá um item de configuração (CI) representando o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior registrado. Para obter mais informações, consulte Frequência de gravação.

  > **Note**
  >
  > AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- Alterar configurações: opcional

Após a configuração, também é possível substituir a frequência de gravação ou excluir tipos de recursos específicos da gravação. Para substituir as configurações padrão, escolha Configurações no painel de navegação à esquerda do AWS Config console e escolha Editar.

Considerações ao registrar recursos

Alto número de AWS Config avaliações

Você pode notar um aumento na atividade em sua conta durante a gravação do mês inicial com o AWS Config em comparação com os meses subsequentes. Durante o processo inicial de inicialização, AWS Config executa avaliações em todos os recursos da sua conta que você selecionou para serem registrados. AWS Config

Se você estiver executando workloads efêmeros, poderá observar um aumento na atividade do AWS Config conforme ele registra as alterações de configuração associadas à criação e exclusão desses recursos temporários. Um workload efêmero é um uso temporário de recursos de computação que são carregados e executados quando necessário. Exemplos incluem instâncias spot do Amazon Elastic Compute Cloud (Amazon EC2), trabalhos do Amazon EMR e o AWS Auto Scaling. Se quiser evitar o aumento da atividade decorrente da execução de cargas de trabalho efêmeras, você pode configurar o gravador de configuração para excluir esses tipos de recursos do registro ou executar esses tipos de cargas de trabalho em uma conta separada, AWS Config desativada, para evitar maiores registros de configuração e avaliações de regras.

Tipos de recursos globais | Os clusters globais do Aurora são inicialmente incluídos na gravação

O tipo de `AWS::RDS::GlobalCluster` recurso será registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado.

Se você não quiser gravar o `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, poderá excluir esse tipo de recurso da gravação após a configuração. Selecione Configurações na barra de navegação esquerda e, depois, escolha Editar. Em Editar, acesse Substituir configurações na seção Método de gravação, selecione `AWS::RDS::GlobalCluster` e escolha a substituição “Excluir da gravação”.

Tipos de recursos globais | Os tipos de recursos do IAM são inicialmente excluídos da gravação

“Todos os tipos de recursos do IAM gravados globalmente” são inicialmente excluídos da gravação para ajudar a reduzir custos. Esse pacote inclui usuários, grupos e perfis do IAM e políticas

gerenciadas pelo cliente. Selecione Remover para remover a substituição e incluir esses recursos na gravação.

A exceção a essa observação refere-se à região do Leste dos EUA (Norte da Virgínia). Os tipos de recursos globais do IAM são inicialmente incluídos na região do Leste dos EUA (Norte da Virgínia), pois essa região funciona como a origem dos tipos de recursos globais do IAM.

Além disso, os tipos globais de recursos do IAM (`AWS::IAM::UserAWS::IAM::Group`,`AWS::IAM::Role`, e`AWS::IAM::Policy`) não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Governança de dados

O período padrão de retenção de AWS Config dados para reter dados por 7 anos (2557 dias) é selecionado para você nesta seção.

A opção Usar uma função AWS Config vinculada ao serviço existente é selecionada para você e definida para a AWS Config função. As funções vinculadas ao serviço são predefinidas AWS Config e incluem todas as permissões que o serviço exige para chamar outros serviços. AWS

Método de entrega

A opção para Selecionar um bucket da conta está selecionada para você nesta seção. Essa seleção usará como padrão o bucket em sua conta que é nomeado no formato`config-bucket-`*`accountid`*. Por exemplo, `config-bucket-012345678901`. Caso você não tenha um bucket criado nesse formato, um será criado para você. Para criar um bucket, consulte Criar um bucket no Guia do usuário do Amazon Simple Storage Service.

Para mais informações sobre os buckets do S3, consulte Visão geral dos buckets no Guia do usuário do Amazon Simple Storage Service.

Regras

Nesta etapa, nenhuma regra é selecionada para você em Regras gerenciadas pela AWS . Em vez disso, recomendamos que você crie e atualize as regras depois de concluir a configuração da conta.

Revisar

Revise seus detalhes de AWS Config configuração. Você pode voltar para editar as alterações em cada seção. Escolha Confirmar para concluir a configuração AWS Config.

Configuração manual

Com o fluxo de trabalho Começar, você pode passar por todas as seleções manuais do processo de configuração para começar a usar o AWS Config console. Para um processo simplificado de introdução, consulte Configuração com 1 clique.

Para configurar AWS Config com o console usando Get started

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Escolha Comece a usar.

A página de configuração inclui três etapas. As informações abaixo apresentam um detalhamento desse processo depois de escolher a opção Comece a usar.

- Configurações: Para selecionar a maneira pela qual o AWS Config console registra recursos e funções e escolher para onde o histórico de configuração e os arquivos instantâneos de configuração são enviados.
- Regras: para regiões que oferecem suporte a regras, esta subseção está disponível para você configurar as regras AWS gerenciadas iniciais que você pode adicionar à sua conta.

  Após a configuração, AWS Config avaliará seus AWS recursos de acordo com as regras que você escolheu. É possível criar regras adicionais e atualizar as existentes em sua conta após a configuração. Para obter mais informações sobre regras, consulte Gerenciando suas AWS Config regras.
- Revisão: Para verificar os detalhes da configuração.

Configurações

Estratégia de gravação

Na seção Método de gravação, selecione uma estratégia de gravação. Você pode especificar os AWS recursos que AWS Config deseja registrar.

All resource types with customizable overrides

Configure AWS Config para registrar as alterações de configuração para todos os tipos de recursos suportados atuais e futuros nesta região. É possível substituir a frequência de gravação

ou excluir tipos de recursos específicos da gravação. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

- Configurações padrão

  Configure a frequência de gravação padrão para todos os tipos de recursos compatíveis atuais e futuros. Para obter mais informações, consulte Frequência de gravação.

  - Gravação contínua — AWS Config registrará as alterações de configuração continuamente sempre que uma alteração ocorrer.
  - Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior registrado.

  > **Note**
  >
  > AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- Configurações de substituição

  Substitua a frequência de gravação ou exclua tipos de recursos específicos da gravação. Se você selecionar a frequência de gravação ou interromper a gravação de um tipo de recurso, os itens de configuração já gravados permanecerão inalterados.

Specific resource types

AWS Config Defina para registrar as alterações de configuração somente para os tipos de recursos que você especificar.

- Tipos de recursos específicos

  Selecione um tipo de recurso a ser gravado e a frequência. Para obter mais informações, consulte Frequência de gravação.

  - Gravação contínua — AWS Config registrará as alterações de configuração continuamente sempre que uma alteração ocorrer.

- Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior registrado.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

Se você selecionar a frequência de gravação ou interromper a gravação de um tipo de recurso, os itens de configuração já gravados permanecerão inalterados.

Considerações ao registrar recursos

Alto número de AWS Config avaliações

Você pode notar um aumento na atividade em sua conta durante a gravação do mês inicial com o AWS Config em comparação com os meses subsequentes. Durante o processo inicial de inicialização, AWS Config executa avaliações em todos os recursos da sua conta que você selecionou para serem registrados. AWS Config

Se você estiver executando workloads efêmeros, poderá observar um aumento na atividade do AWS Config conforme ele registra as alterações de configuração associadas à criação e exclusão desses recursos temporários. Um workload efêmero é um uso temporário de recursos de computação que são carregados e executados quando necessário. Os exemplos incluem instâncias spot do Amazon Elastic Compute Cloud (Amazon EC2), trabalhos do Amazon EMR e. AWS Auto Scaling Se quiser evitar o aumento da atividade decorrente da execução de cargas de trabalho efêmeras, você pode configurar o gravador de configuração para excluir esses tipos de recursos do registro ou executar esses tipos de cargas de trabalho em uma conta separada, AWS Config desativada, para evitar maiores registros de configuração e avaliações de regras.

Considerations: All resource types with customizable overrides

Tipos de recursos gravados globalmente | Os clusters globais do Aurora são inicialmente incluídos na gravação

O tipo de `AWS::RDS::GlobalCluster` recurso será registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado.

Se você não quiser gravar o `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, selecione “AWS RDS GlobalCluster” e escolha a substituição “Excluir da gravação”.

Tipos de recursos globais | Os tipos de recursos do IAM são inicialmente excluídos da gravação

Os tipos de recursos globais do IAM são inicialmente excluídos da gravação para ajudar você a reduzir custos. Esse pacote inclui usuários, grupos e perfis do IAM e políticas gerenciadas pelo cliente. Selecione Remover para remover a substituição e incluir esses recursos na gravação.

A exceção é para o Leste dos EUA (Norte da Virgínia). Os tipos de recursos globais do IAM são inicialmente incluídos na região do Leste dos EUA (Norte da Virgínia), pois essa região funciona como a origem dos tipos de recursos globais do IAM.

Além disso, os tipos globais de recursos do IAM (`AWS::IAM::User``AWS::IAM::Group`,`AWS::IAM::Role`, e`AWS::IAM::Policy`) não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Limites

É possível adicionar até cem substituições de frequência e seiscentas substituições de exclusão.

A gravação diária não é compatível com os seguintes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

Disponibilidade de regiões

Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você AWS Config configurou. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões

suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você configurou AWS Config.

Limites

Não haverá limites se todos os tipos de recursos tiverem a mesma frequência. Será possível adicionar até cem tipos de recursos com frequência diária se pelo menos um tipo de recurso estiver definido como Contínua.

A frequência diária não é compatível com os seguintes tipos de recursos:

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Governança de dados

- Para Período de retenção de dados, escolha o período de retenção padrão para reter AWS Config dados por 7 anos (2557) ou defina um período de retenção personalizado para itens registrados por. AWS Config

  AWS Config permite que você exclua seus dados especificando um período de retenção para seus`ConfigurationItems`. Quando você especifica um período de retenção, AWS Config retém o seu `ConfigurationItems` por esse período especificado. Você pode escolher um período entre um mínimo de 30 dias e um máximo de 7 anos (2557 dias). AWS Config exclui dados mais antigos do que o período de retenção especificado.
- Para a função do IAM para AWS Config, escolha uma função AWS Config vinculada ao serviço existente ou uma função do IAM na sua conta.
  - As funções vinculadas ao serviço são predefinidas AWS Config e incluem todas as permissões que o serviço exige para chamar outros serviços. AWS

> **Note**
>
> Recomendado: use a função vinculada ao serviço
> É recomendável usar a função vinculada ao serviço. Uma função vinculada ao serviço adiciona todas as permissões necessárias AWS Config para ser executada conforme o esperado.

- Caso contrário, escolha uma função do IAM a partir de uma de suas funções e políticas de permissão preexistentes.

> **Note**
>
> Políticas de autorização para evitar AWS Organizations acessos
> Se você usa uma função preexistente do IAM, verifique se não há uma política de autorização AWS Organizations que impeça a permissão AWS Config de registrar seus recursos. Para obter mais informações sobre políticas de autorização para AWS Organizations, consulte Gerenciamento de políticas AWS Organizations no Guia AWS Organizations do usuário.
> Mantenha as permissões mínimas ao reutilizar uma função do IAM
> Se você usa um AWS serviço que usa AWS Config, como AWS Security Hub ou AWS Control Tower, e uma função do IAM já foi criada, certifique-se de que a função do IAM que você usa durante a configuração AWS Config mantenha as mesmas permissões mínimas da função preexistente do IAM. Você deve fazer isso para garantir que o outro AWS serviço continue funcionando conforme o esperado.
> Por exemplo, se AWS Control Tower tiver uma função do IAM que AWS Config permite ler objetos do S3, certifique-se de que as mesmas permissões sejam concedidas à função do IAM que você usa ao configurar AWS Config. Caso contrário, isso pode interferir na forma como AWS Control Tower opera.

Método de entrega

- Para o Método de entrega, escolha o bucket do S3 para o qual o AWS Config envia arquivos de histórico de configuração e de snapshot de configuração:
  - Criar um bucket: para definir o nome do bucket do S3, digite um nome para o seu bucket do S3.

    O nome digitado deve ser exclusivo para todos os nomes de bucket existentes no Amazon S3. Uma forma de ajudar a garantir a exclusividade é incluir um prefixo; por exemplo, o nome de sua organização. Você não pode alterar o nome do bucket após sua criação. Para obter mais informações, consulte Restrições e limitações de bucket no Manual do usuário do Amazon Simple Storage Service.
  - Selecionar um bucket de sua conta: em Nome do bucket do S3, escolha seu bucket de preferência.
  - Selecionar um bucket de outra conta: em Nome do bucket do S3, digite o nome do bucket.

> **Note**
>
> Permissões do bucket
>
> Se você escolher um bucket de outra conta, esse bucket deverá ter políticas que concedam permissões de acesso AWS Config a. Para ter mais informações, consulte Permissões para o bucket Amazon S3 para o AWS Config canal de entrega.

- Para o tópico do Amazon SNS, escolha Transmitir alterações e notificações de configuração para um tópico do Amazon SNS para AWS Config enviar notificações, como entrega de histórico de configuração, entrega de snapshots de configuração e conformidade.
- Se você optar por AWS Config transmitir para um tópico do Amazon SNS, escolha o tópico de destino:
  - Criar um tópico: em Nome do tópico, digite um nome para o tópico do SNS.
  - Escolher um tópico da sua conta: em Nome do tópico, selecione seu tópico de preferência.
  - Escolher um tópico de outra conta: em ARN do tópico, digite o nome do recurso da Amazon (ARN) do tópico. Se você escolher um tópico de outra conta, o tópico deverá ter políticas que concedam permissões de acesso AWS Config a. Para ter mais informações, consulte Permissões para o tópico do Amazon SNS.

> **Note**
>
> Região para o tópico do Amazon SNS
>
> O tópico do Amazon SNS deve existir na mesma região da região na qual você configurou. AWS Config

Regras

Se você estiver configurando AWS Config em uma região que ofereça suporte a regras, escolha Avançar. Para ter mais informações, consulte Adicionando, atualizando e excluindo regras AWS Config.

Caso contrário, selecione Confirmar.

Revisar

Revise seus detalhes de AWS Config configuração. Você pode voltar para editar as alterações em cada seção. Escolha Confirmar para concluir a configuração AWS Config.

Para obter mais informações

Para obter informações sobre a pesquisa de recursos existentes em sua conta e entender as configurações de seus recursos, consulte Exibir histórico e configurações de recursos da .

Você também pode usar o Amazon Simple Queue Service para monitorar AWS recursos de forma programática. Para ter mais informações, consulte Monitorando mudanças AWS de recursos com o Amazon SQS.

Configurando AWS Config com o AWS CLI

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, insira `aws configure` para configurar o AWS CLI para usar uma AWS região onde AWS Config esteja disponível.

Configuração

Consulte os tópicos a seguir para configurar AWS Config com AWS CLI o.

Tópicos

- Pré-requisitos
- Começando AWS Config com o AWS CLI
- Verificando se foi AWS Config iniciado com sucesso com o AWS CLI

Pré-requisitos

Antes de configurar AWS com o AWS CLI, você precisa criar um bucket do Amazon S3, um tópico do Amazon SNS e uma função do IAM com políticas anexadas como pré-requisitos. Em seguida, você pode usar o AWS CLI para especificar o bucket, o tópico e a função do AWS Config. Siga este procedimento para configurar seus pré-requisitos para o AWS Config.

Sumário

- Criando um Bucket do Amazon S3
- Criar um tópico do Amazon SNS
- Criar um perfil do IAM

Criando um Bucket do Amazon S3

Se você já tem um bucket do S3 em sua conta e deseja usá-lo, ignore esta etapa e vá para Criar um tópico do Amazon SNS.

Uso do console do S3

Para criar um bucket

1. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Selecione Criar bucket.
3. Em Bucket name (Nome do bucket), insira um nome compatível com o DNS para seu bucket.

   O nome do bucket deve:

   - Seja exclusivo em todo o Amazon S3.
   - Ter entre 3 e 63 caracteres.
   - Não contém caracteres maiúsculos.
   - Começar com uma letra minúscula ou um número.

   Depois de criado o bucket, você não pode mudar seu nome. Garanta que o nome do bucket escolhido seja exclusivo entre todos os nomes de buckets existentes no Amazon S3. Para obter mais informações sobre as regras e convenções de nomeação buckets, consulte Restrições e limitações de buckets no Guia do usuário do Amazon Simple Storage Service.

> **Important**
>
> Evite incluir informações confidenciais no nome do bucket. O nome do bucket é visível nos URLs que apontam para os objetos no bucket.

4. Em Região, escolha a AWS região em que você deseja que o bucket resida.

   Escolha uma região próxima de você para minimizar a latência e os custos e atender aos requisitos regulatórios. Os objetos armazenados em uma região nunca saem dessa região, a menos que você os transfira para outra região. Para obter uma lista das AWS regiões do Amazon S3, consulte os endpoints AWS de serviço no. Referência geral da Amazon Web Services

5. Em Bucket settings for Block Public Access (Configurações de bucket para o Bloqueio de acesso público), escolha as configurações de bloqueio de acesso público que deseja aplicar ao bucket.

   Recomendamos que você deixe todas as configurações ativadas, a menos que saiba que precisa desativar uma ou mais delas para seu caso de uso, como para hospedar um site público. As configurações de bloqueio de acesso público que você habilitar para o bucket também serão ativadas para todos os pontos de acesso criados no bucket. Para obter mais informações sobre como bloquear o acesso público, consulte Usar o bloqueio de acesso público do Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

6. (Opcional) Se você quiser ativar o bloqueio de objetos do S3:

   a. Escolha Advanced settings (Configurações avançadas) e leia a mensagem exibida.

   > **Important**
   >
   > Você só pode habilitar o bloqueio de objetos do S3 para um bucket ao criá-lo. Se você habilitar o bloqueio de objetos para o bucket, não poderá desabilitá-lo mais tarde. A ativação do bloqueio de objetos também permite o versionamento para o bucket. Depois de habilitar o bloqueio de objetos para o bucket, você deve definir as configurações de bloqueio de objetos antes que qualquer objeto no bucket seja protegido. Para obter mais informações sobre como configurar a proteção de objetos, consulte Configurar o bloqueio de objetos do S3 usando o console do Amazon S3.

b. Se quiser ativar o bloqueio de objetos, insira enable na caixa de texto e escolha Confirm (Confirmar).

Para obter mais informações sobre o recurso Bloqueio de Objetos do S3, consulte Usar o bloqueio de objetos do S3 no Guia do usuário do Amazon Simple Storage Service.

7. Selecione Criar bucket.

Usando os AWS SDKs

Ao usar os AWS SDKs para criar um bucket, você deve criar um cliente e, em seguida, usar o cliente para enviar uma solicitação para criar um bucket. Como prática recomendada, crie o cliente e o bucket na mesma Região da AWS. Se você não especificar uma região ao criar um cliente ou um bucket, o Amazon S3 usará a região padrão Leste dos EUA (Norte da Virgínia).

Para criar um cliente para acessar um endpoint de pilha dupla, você deve especificar um. Região da AWS Para obter mais informações, consulte Endpoints de pilha dupla do Amazon S3. Para obter uma lista dos disponíveis Regiões da AWS, consulte Regiões e endpoints no Referência geral da AWS.

Ao criar um cliente, a região mapeia para o endpoint específico da região. O cliente usa esse endpoint para se comunicar com o Amazon S3: `s3.<region>.amazonaws.com`. Se a sua região foi lançada após 20 de março de 2019,, seu cliente e bucket devem estar na mesma região. No entanto, é possível usar um cliente na região Leste dos EUA (Norte da Virgínia) para criar um bucket em qualquer região iniciada antes de 20 de março de 2019. Para obter mais informações, consulte Endpoints herdados.

Esses exemplos de código do AWS SDK realizam as seguintes tarefas:

- Crie um cliente especificando explicitamente uma região da Região da AWS: no exemplo, o cliente usa o endpoint `s3.us-west-2.amazonaws.com` para se comunicar com o Amazon S3. É possível especificar qualquer Região da AWS. Para obter uma lista de Regiões da AWS, consulte Regiões e endpoints na Referência AWS geral.
- Envie uma solicitação de bucket de criação especificando apenas um nome de bucket — O cliente envia uma solicitação ao Amazon S3 para criar o bucket na região onde você criou um cliente.
- Recupere as informações sobre a localização do bucket. O Amazon S3 armazena as informações de localização do bucket no sub-recurso location que está associado ao bucket.

Os exemplos de códigos a seguir mostram como usar `CreateBucket`.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
                return false;
            }
        }
```

Crie um bucket com o bloqueio de objetos habilitado.

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for .NET da API.

Bash

AWS CLI com script Bash

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
###############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
###############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
```

```
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi
```

```
  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- Para obter detalhes da API, consulte CreateBucketna Referência de AWS CLI Comandos.

C++

SDK para C++

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
bool AwsDoc::S3::CreateBucket(const Aws::String &bucketName,
                              const Aws::Client::ClientConfiguration
 &clientConfig) {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    //TODO(user): Change the bucket location constraint enum to your target
 Region.
    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: CreateBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    }
    else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for C++ da API.

CLI

AWS CLI

Exemplo 1: como criar um bucket

O seguinte exemplo de `create-bucket` cria um bucket chamado `my-bucket`:

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1
```

Saída:

```
{
    "Location": "/my-bucket"
}
```

Para obter mais informações, consulte Como criar um bucket no Guia do usuário do Amazon S3.

Exemplo 2: como criar um bucket com aplicação de políticas de proprietário

O exemplo de `create-bucket` a seguir cria um bucket chamado `my-bucket` que usa a configuração aplicada de proprietário de bucket para a propriedade de objetos do S3.

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

Saída:

```
{
    "Location": "/my-bucket"
}
```

Para obter mais informações, consulte Controlar a propriedade de objetos e desabilitar ACLs, no Guia do usuário do Amazon S3.

Exemplo 3: como criar um bucket fora da região ``us-east-1``

O exemplo de `create-bucket` a seguir cria um bucket chamado `my-bucket` na região `eu-west-1`. Regiões fora da `us-east-1` exigem que o `LocationConstraint` adequado seja especificado para poder criar o bucket na região desejada.

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region eu-west-1 \
```

```
    --create-bucket-configuration LocationConstraint=eu-west-1
```

Saída:

```
{
    "Location": "http://my-bucket.s3.amazonaws.com/"
}
```

Para obter mais informações, consulte Como criar um bucket no Guia do usuário do Amazon S3.

- Para obter detalhes da API, consulte CreateBucketna Referência de AWS CLI Comandos.

Go

SDK para Go V2

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(name string, region string) error {
 _, err := basics.S3Client.CreateBucket(context.TODO(), &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
```

```
    LocationConstraint: types.BucketLocationConstraint(region),
   },
  })
  if err != nil {
   log.Printf("Couldn't create bucket %v in Region %v. Here's why: %v\n",
    name, region, err)
  }
  return err
}
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for Go da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie um bucket.

```
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.waiters.S3Waiter;
import java.net.URISyntaxException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateBucket {
    public static void main(String[] args) throws URISyntaxException {
        final String usage = """

                Usage:
                    <bucketName>\s

                Where:
                    bucketName - The name of the bucket to create. The bucket
 name must be unique, or an error occurs.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String bucketName = args[0];
        System.out.format("Creating a bucket named %s\n", bucketName);
        Region region = Region.US_EAST_1;
        S3Client s3 = S3Client.builder()
                .region(region)
                .build();

        createBucket(s3, bucketName);
        s3.close();
    }

    public static void createBucket(S3Client s3Client, String bucketName) {
        try {
            S3Waiter s3Waiter = s3Client.waiter();
            CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            s3Client.createBucket(bucketRequest);
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                    .bucket(bucketName)
                    .build();
```

```
            // Wait until the bucket is created and print out the response.
            WaiterResponse<HeadBucketResponse> waiterResponse =
 s3Waiter.waitUntilBucketExists(bucketRequestWait);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println(bucketName + " is ready");

        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

Crie um bucket com o bloqueio de objetos habilitado.

```
    // Create a new Amazon S3 bucket with object lock options.
    public void createBucketWithLockOptions(boolean enableObjectLock, String
 bucketName) {
        S3Waiter s3Waiter = getClient().waiter();
        CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectLockEnabledForBucket(enableObjectLock)
            .build();

        getClient().createBucket(bucketRequest);
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie o bucket.

```
import { CreateBucketCommand, S3Client } from "@aws-sdk/client-s3";

const client = new S3Client({});

export const main = async () => {
  const command = new CreateBucketCommand({
    // The name of the bucket. Bucket names are unique and have several other
 constraints.
    // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
    Bucket: "bucket-name",
  });

  try {
    const { Location } = await client.send(command);
    console.log(`Bucket created with location ${Location}`);
  } catch (err) {
    console.error(err);
  }
};
```

- Para obter mais informações, consulte o Guia do desenvolvedor do AWS SDK for JavaScript.
- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for JavaScript da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- Para obter detalhes da API, consulte a CreateBucketreferência da API AWS SDK for Kotlin.

PHP

SDK para PHP

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie um bucket.

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
```

```
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for PHP da API.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie um bucket com as configurações padrão.

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
```

```
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

Crie um bucket versionado com uma configuração de ciclo de vida.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
```

```
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- Para obter detalhes da API, consulte a CreateBucketReferência da API AWS SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
require "aws-sdk-s3"

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
```

```
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get its location!"
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("doc-example-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

- Para obter detalhes da API, consulte CreateBucketa Referência AWS SDK for Ruby da API.

Rust

SDK para Rust

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
pub async fn create_bucket(
    client: &Client,
    bucket_name: &str,
    region: &str,
) -> Result<CreateBucketOutput, SdkError<CreateBucketError>> {
    let constraint = BucketLocationConstraint::from(region);
    let cfg = CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await
}
```

- Para obter detalhes da API, consulte a CreateBucketreferência da API AWS SDK for Rust.

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
TRY.
    lo_s3->createbucket(
        iv_bucket = iv_bucket_name
    ).
    MESSAGE 'S3 bucket created.' TYPE 'I'.
  CATCH /aws1/cx_s3_bucketalrdyexists.
    MESSAGE 'Bucket name already exists.' TYPE 'E'.
  CATCH /aws1/cx_s3_bktalrdyownedbyyou.
    MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
ENDTRY.
```

- Para obter detalhes da API, consulte a CreateBucketreferência da API AWS SDK for SAP ABAP.

Swift

SDK para Swift

> **Note**
>
> Esta é a documentação de pré-lançamento de um SDK na versão de visualização. Está sujeita a alteração.

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    public func createBucket(name: String) async throws {
        let config = S3ClientTypes.CreateBucketConfiguration(
            locationConstraint: .usEast2
        )
        let input = CreateBucketInput(
            bucket: name,
            createBucketConfiguration: config
        )
        _ = try await client.createBucket(input: input)
    }
```

- Para obter detalhes da API, consulte CreateBucketa referência da API AWS SDK for Swift.

> **Note**
>
> Você também pode usar um bucket do Amazon S3 de uma conta diferente, mas pode ser necessário criar uma política para o bucket que conceda permissões de acesso para o AWS Config. Para obter informações sobre a concessão de permissões para um bucket do S3, consulte Permissões para o bucket Amazon S3 para o AWS Config canal de entrega e, em seguida, vá para Criar um tópico do Amazon SNS.

Criar um tópico do Amazon SNS

Se você já tem um tópico do Amazon SNS em sua conta e deseja usá-lo, ignore esta etapa e vá para Criar um perfil do IAM.

Como usar o console do SNS

Para criar um tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Execute um destes procedimentos:
   - Se nenhum tópico já tiver sido criado Conta da AWS antes, leia a descrição do Amazon SNS na página inicial.

- Se os tópicos já tiverem sido criados abaixo Conta da AWS do seu, no painel de navegação, escolha Tópicos.

3. Na página Topics (Tópicos), escolha Create topic (Criar tópico).
4. Na página Create topic (Criar tópico), na seção Details (detalhes), faça o seguinte:

   a. Em Type (Tipo), escolha um tipo de tópico (Standard (Padrão) ou FIFO).

   b. Insira um Name (Nome) para o tópico. Para um tópico FIFO, adicione .fifo ao final do nome.

   c. (Opcional) Insira um Display name (Nome para exibição) para o tópico.

   d. (Opcional) Para um tópico FIFO, você pode escolher content-based message deduplication (Desduplicação de mensagens baseada em conteúdo) para habilitar a desduplicação de mensagens padrão. Para obter mais informações, consulte Desduplicação de mensagens para tópicos FIFO.

5. (Opcional) Expanda a seção Encryption (Criptografia) e faça o seguinte. Para obter mais informações, consulte Criptografia em repouso.

   a. Selecione Ativar criptografia.

   b. Especifique a chave mestra de cliente (CMK). Para obter mais informações, consulte Termos de chaves.

      Para cada tipo de CMK, a Description (Descrição), a Account (Conta) e o CMK ARN (ARN da CMK) são exibidos.

      > **Important**
      >
      > Se você não for o proprietário da CMK ou se fizer login com uma conta que não tenha permissões `kms:ListAliases` e `kms:DescribeKey`, não será possível visualizar as informações sobre a CMK no console do Amazon SNS.
      > Peça ao proprietário da CMK para conceder essas permissões a você. Para obter mais informações, consulte AWS KMS API Permissions: Actions and Resources Reference (“Permissões da API do KMS: referência de ações e recursos”) no Guia do desenvolvedor do AWS Key Management Service .

      - O alias/aws/sns (padrão) da CMK AWS gerenciada para Amazon SNS é selecionado por padrão.

> **Note**
>
> Lembre-se do seguinte:
>
> - A primeira vez que você usa o AWS Management Console para especificar a CMK AWS gerenciada para o Amazon SNS para um tópico AWS KMS , cria a CMK gerenciada para AWS o Amazon SNS.
> - Como alternativa, na primeira vez em que você usa a `Publish` ação em um tópico com o SSE ativado, AWS KMS cria a CMK AWS gerenciada para o Amazon SNS.

- Para usar uma CMK personalizada da sua Conta da AWS, escolha o campo Chave mestra do cliente (CMK) e, em seguida, escolha a CMK personalizada na lista.

> **Note**
>
> Para obter instruções sobre como criar CMKs personalizadas, consulte Creating Keys (“Criar chaves”) no Guia do desenvolvedor do AWS Key Management Service .

- Para usar um ARN de CMK personalizado da Conta da AWS sua conta ou de AWS outra conta, insira-o no campo Chave mestra do cliente (CMK).

6. (Opcional) Por padrão, somente o proprietário do tópico pode publicar ou assinar o tópico. Para configurar permissões de acesso adicionais, expanda a seção Política de acesso. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Amazon SNS e Casos de exemplo do controle de acesso do Amazon SNS.

> **Note**
>
> Quando você cria um tópico usando o console, a política padrão usa a chave de condição `aws:SourceOwner`. Essa chave é semelhante a `aws:SourceAccount`.

7. (Opcional) Para configurar como o Amazon SNS repete tentativas de entrega de mensagem com falha, expanda a seção Delivery retry policy (HTTP/S) (Política de repetição de entrega (HTTP/S)). Para obter mais informações, consulte Novas tentativas de entrega de mensagens do Amazon SNS.

8. (Opcional) Para configurar como o Amazon SNS registra a entrega de mensagens CloudWatch, expanda a seção Registro de status de entrega. Para obter mais informações, consulte Status de entrega de mensagens do Amazon SNS.
9. (Opcional) Para adicionar tags de metadados ao tópico, expanda a seção Tags, insira uma Key (chave) e um Value (Valor) (opcional) e escolha Add tag (Adicionar tag). Para obter mais informações, consulte Marcação de tópicos do Amazon SNS.
10. Escolha Criar tópico.

    O tópico é criado e a ***MyTopic***página é exibida.

    O Name (Nome), o ARN e o Display name (Nome de exibição) (opcional) do tópico, além do ID da conta da AWS do Topic owner (Proprietário do tópico) são exibidos na seção Details (Detalhes).
11. Copie o ARN do tópico para a área de transferência, por exemplo:

    ```
    arn:aws:sns:us-east-2:123456789012:MyTopic
    ```

Como inscrever um endereço de e-mail no tópico do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. No painel de navegação à esquerda, escolha Assinaturas.
3. Na página Subscriptions (Assinaturas), escolha Create subscription (Criar assinatura).
4. Na página Create subscription (Criar inscrição), na seção Details (detalhes), faça o seguinte:

   a. Em Topic ARN (ARN do tópico), escolha o nome do recurso da Amazon (ARN) de um tópico.

   b. Em Protocol (Protocolo), escolha um tipo de endpoint. Os tipos de endpoint disponíveis são:

      - HTTP/HTTPS
      - Email/Email-JSON
      - Amazon Data Firehose
      - Amazon SQS

> **Note**
>
> Para se inscrever em um tópico FIFO do SNS, escolha esta opção.

- AWS Lambda
- Endpoint da aplicação da plataforma
- SMS

c. Em Endpoint, insira o valor do endpoint, como um endereço de e-mail ou o ARN de uma fila do Amazon SQS.

d. Somente endpoints do Firehose: para o ARN da função de assinatura, especifique o ARN da função do IAM que você criou para gravar nos fluxos de entrega do Firehose. Para obter mais informações, consulte Pré-requisitos para inscrever streams de entrega do Firehose nos tópicos do Amazon SNS.

e. (Opcional) Para endpoints Firehose, Amazon SQS e HTTP/S, você também pode ativar a entrega de mensagens brutas. Para obter mais informações, consulte Entrega de mensagens brutas do Amazon SNS.

f. (Opcional) Para configurar uma política de filtros, expanda a seção Subscription filter policy (Política de filtro de assinatura). Para obter mais informações, consulte Políticas de filtro de assinatura do Amazon SNS.

g. (Opcional) Para configurar uma fila de mensagens mortas para a assinatura, expanda a seção Redrive policy (dead-letter queue) (Política de redirecionamento (fila de mensagens mortas)). Para obter mais informações, consulte Filas de mensagens não entregues (DLQs) do Amazon SNS.

h. Selecione Criar assinatura.

   O console cria a assinatura e abre a página Details (Detalhes) da assinatura.

Usando os AWS SDKs

Para usar um AWS SDK, você deve configurá-lo com suas credenciais. Para obter mais informações, consulte The shared config and credentials files (“Os arquivos compartilhados de configuração e de credenciais”) no Guia de referência de AWS SDKs e ferramentas.

Os exemplos de códigos a seguir mostram como usar `CreateTopic`.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie um tópico com um nome específico.

```
    using System;
    using System.Threading.Tasks;
    using Amazon.SimpleNotificationService;
    using Amazon.SimpleNotificationService.Model;

    /// <summary>
    /// This example shows how to use Amazon Simple Notification Service
    /// (Amazon SNS) to add a new Amazon SNS topic.
    /// </summary>
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

            var topicArn = await CreateSNSTopicAsync(client, topicName);
            Console.WriteLine($"New topic ARN: {topicArn}");
        }

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
```

```
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

Crie um tópico com um nome e atributos específicos de FIFO e desduplicação.

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }
```

```
            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for .NET da API.

C++

SDK para C++

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
```

```
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for C++ da API.

CLI

AWS CLI

Para criar um tópico do SNS

O exemplo `create-topic` a seguir cria um tópico do SNS chamado `my-topic`.

```
aws sns create-topic \
    --name my-topic
```

Saída:

```
{
    "ResponseMetadata": {
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
```

```
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

Para obter mais informações, consulte Usando a interface de linha de AWS comando com o Amazon SQS e o Amazon SNS no Guia do usuário AWS da interface de linha de comando.

- Para obter detalhes da API, consulte CreateTopicna Referência de AWS CLI Comandos.

Go

SDK para Go V2

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(topicName string, isFifoTopic bool,
 contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
```

```
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(context.TODO(), &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for Go da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

        } catch (SnsException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
```

```
        }
        return "";
    }
}
```

- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no AWS Code Examples Repository.

Crie o cliente em um módulo separado e exporte-o.

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

Importe o SDK e os módulos do cliente e chame a API.

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
```

```
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- Para obter mais informações, consulte o Guia do desenvolvedor do AWS SDK for JavaScript.
- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for JavaScript da API.

Kotlin

SDK para Kotlin

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
        CreateTopicRequest {
            name = topicName
        }

    SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
    }
```

```
}
```

- Para obter detalhes da API, consulte a CreateTopicreferência da API AWS SDK for Kotlin.

PHP

SDK para PHP

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
require 'vendor/autoload.php';

use Aws\Exception\AwsException;
use Aws\Sns\SnsClient;


/**
 * Create a Simple Notification Service topics in your AWS account at the
 requested region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
```

```
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- Para obter mais informações, consulte o Guia do desenvolvedor do AWS SDK for PHP.
- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for PHP da API.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource


    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
```

```
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- Para obter detalhes da API, consulte a CreateTopicReferência da API AWS SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e saiba como configurar e executar no Repositório de exemplos de código da AWS.

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
```

```
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = "YourTopicName" # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts "The topic was not created. Stopping program."
    exit 1
  end
end
```

- Para obter mais informações, consulte o Guia do desenvolvedor do AWS SDK for Ruby.
- Para obter detalhes da API, consulte CreateTopica Referência AWS SDK for Ruby da API.

Rust

SDK para Rust

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
```

```
}
```

- Para obter detalhes da API, consulte a CreateTopicreferência da API AWS SDK for Rust.

SAP ABAP

SDK para SAP ABAP

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
   TRY.
       oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
is returned for testing purposes. "
       MESSAGE 'SNS topic created' TYPE 'I'.
     CATCH /aws1/cx_snstopiclimitexcdex.
       MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- Para obter detalhes da API, consulte a CreateTopicreferência da API AWS SDK for SAP ABAP.

> **Note**
>
> Você também pode usar um tópico do Amazon SNS em uma conta diferente, mas nesse caso, pode ser necessário criar uma política para o tópico que conceda permissões de acesso para o AWS Config. Para informações sobre a concessão de permissões para um tópico do Amazon SNS, consulte Permissões para o tópico do Amazon SNS e, em seguida, vá para Criar um perfil do IAM.

Criar um perfil do IAM

Como usar o console do IAM

Você pode usar o console do IAM para criar uma função do IAM que concede AWS Config permissões para acessar seu bucket do Amazon S3, acessar seu tópico do Amazon SNS e obter detalhes de configuração dos recursos compatíveis. AWS Quando você usa o console para criar um perfil do IAM, o AWS Config associa automaticamente as permissões necessárias ao perfil para você.

> **Note**
>
> Se você usou um AWS serviço que usa AWS Config (como AWS Security Hub ou AWS Control Tower) e uma AWS Config função já foi criada, certifique-se de que a função do IAM usada durante a configuração AWS Config mantenha os mesmos privilégios mínimos da AWS Config função já criada para que o outro AWS serviço continue funcionando conforme o esperado.
> Por exemplo, se o AWS Control Tower tiver uma função do IAM que AWS Config permite ler objetos do Amazon S3, você deve garantir que as mesmas permissões sejam concedidas dentro da função do IAM que você usa ao configurar. AWS Config Caso contrário, isso pode interferir nas operações da Torre de AWS Controle.
> Para obter mais informações sobre as funções do IAM para AWS Config, consulte AWS Identity and Access Management.

Para criar uma função para um AWS serviço

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Roles (Perfis) e, em seguida, Create role (Criar perfil).
3. Em Select trusted entity (Selecionar entidade confiável), escolha AWS Service (Serviço).
4. Escolha o caso de uso que você deseja para AWS Config: Config - Customizable, Config - Organizations, Config ou Config - Conformance Packs. Em seguida, escolha Próximo.
5. Na página Nomear, revisar e criar, analise os detalhes do perfil e selecione Criar perfil.

Usando os AWS SDKs

Para usar um AWS SDK, você deve configurá-lo com suas credenciais. Para obter mais informações, consulte The shared config and credentials files ("Os arquivos compartilhados de configuração e de credenciais") no Guia de referência de AWS SDKs e ferramentas.

Os exemplos de códigos a seguir mostram como usar `CreateRole`.

.NET

AWS SDK for .NET

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role.</param>
    /// <param name="rolePolicyDocument">The name of the IAM policy document
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for .NET da API.

Bash

AWS CLI com script Bash

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
###############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
###############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

###############################################################################
# function iam_create_role
#
# This function creates an IAM role.
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
```

```
  echo "  -n role_name   The name of the IAM role."
  echo "  -p policy_json -- The assume role policy document."
  echo ""
}

# Retrieve the calling parameters.
while getopts "n:p:h" option; do
  case "${option}" in
    n) role_name="${OPTARG}" ;;
    p) policy_document="${OPTARG}" ;;
    h)
      usage
      return 0
      ;;
    \?)
      echo "Invalid parameter"
      usage
      return 1
      ;;
  esac
done
export OPTIND=1

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

if [[ -z "$policy_document" ]]; then
  errecho "ERROR: You must provide a policy document with the -p parameter."
  usage
  return 1
fi

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
  --query Role.Arn)

local error_code=${?}

if [[ $error_code -ne 0 ]]; then
```

```
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- Para obter detalhes da API, consulte CreateRolena Referência de AWS CLI Comandos.

C++

SDK para C++

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
```

```
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for C++ da API.

CLI

AWS CLI

Exemplo 1: como criar um perfil do IAM

O comando `create-role`, apresentado a seguir, cria um perfil, denominado `Test-Role`, e anexa uma política de confiança a ele.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

Saída:

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

A política de confiança é definida como um documento JSON no arquivo Test-Role-Trust-Policy.json. (O nome e a extensão do arquivo não têm significado.) A política de confiança deve especificar uma entidade principal.

Para anexar uma política de permissões a um perfil, use o comando `put-role-policy`.

Para obter mais informações, consulte Criação de perfis do IAM no Guia do usuário do AWS IAM.

Exemplo 2: como criar um perfil do IAM com a duração máxima da sessão especificada

O comando `create-role`, apresentado a seguir, cria um perfil denominado `Test-Role` e define a duração máxima da sessão como 7.200 segundos (duas horas).

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

Saída:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Para obter mais informações, consulte Modificar a duração máxima da sessão (AWS API) de uma função no Guia do usuário do AWS IAM.

Exemplo 3: como criar um perfil do IAM com etiquetas

O comando apresentado a seguir cria um perfil do IAM `Test-Role` com etiquetas. Este exemplo usa o sinalizador de parâmetro `--tags` com as seguintes etiquetas formatadas em JSON: `'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'`. Como alternativa, o sinalizador `--tags` pode ser usado com etiquetas no formato abreviado: `'Key=Department,Value=Accounting Key=Location,Value=Seattle'`.

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

Saída:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
```

```
                "Value": "Seattle"
            }
        ]
    }
}
```

Para obter mais informações, consulte Marcar perfis do IAM no Guia do usuário do AWS IAM.

- Para obter detalhes da API, consulte CreateRolena Referência de AWS CLI Comandos.

Go

SDK para Go V2

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(roleName string, trustedUserArn string)
 (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version:   "2012-10-17",
  Statement: []PolicyStatement{{
```

```
    Effect: "Allow",
    Principal: map[string]string{"AWS": trustedUserArn},
    Action: []string{"sts:AssumeRole"},
   }},
  }
  policyBytes, err := json.Marshal(trustPolicy)
  if err != nil {
   log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
  trustedUserArn, err)
   return nil, err
  }
  result, err := wrapper.IamClient.CreateRole(context.TODO(),
  &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(string(policyBytes)),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  } else {
   role = result.Role
  }
  return role, err
 }
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for Go da API.

Java

SDK para Java 2.x

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
```

```
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
 represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
```

```
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
 fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
 readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

            CreateRoleResponse response = iam.createRole(request);
            System.out.println("The ARN of the role is " +
 response.role().arn());

        } catch (IamException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return "";
    }

    public static Object readJsonSimpleDemo(String filename) throws Exception {
        FileReader reader = new FileReader(filename);
        JSONParser jsonParser = new JSONParser();
        return jsonParser.parse(reader);
    }
}
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for Java 2.x da API.

JavaScript

SDK para JavaScript (v3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

Crie a função.

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for JavaScript da API.

PHP

SDK para PHP

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
$uuid = uniqid();
$service = new IAMService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
```

```
            ]);
        });
        return $result['Role'];
    }
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for PHP da API.

PowerShell

Ferramentas para PowerShell

Exemplo 1: este exemplo cria um perfil denominado **MyNewRole** e anexa a ele a política encontrada no arquivo **NewRoleTrustPolicy.json**. Observe que você deve usar o parâmetro switch **-Raw** para processar com êxito o arquivo de política JSON. O documento de política exibido na saída é codificado em URL. Ele é decodificado nesse exemplo com o método .NET **UrlDecode**.

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

Saída:

```
Arn                      : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
```

```
RoleId                    : V5PAJI2KPN4EAEXAMPLE1
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- Para obter detalhes da API, consulte CreateRoleem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.

    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
```

```
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Principal": {"Service": service},
                "Action": "sts:AssumeRole",
            }
            for service in allowed_services
        ],
    }

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- Para obter detalhes da API, consulte a CreateRoleReferência da API AWS SDK for Python (Boto3).

Ruby

SDK para Ruby

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
# Creates a role and attaches policies to it.
#
# @param role_name [String] The name of the role.
```

```
  # @param assume_role_policy_document [Hash] The trust relationship policy
 document.
  # @param policy_arns [Array<String>] The ARNs of the policies to attach.
  # @return [String, nil] The ARN of the new role if successful, or nil if an
 error occurred.
  def create_role(role_name, assume_role_policy_document, policy_arns)
    response = @iam_client.create_role(
      role_name: role_name,
      assume_role_policy_document: assume_role_policy_document.to_json
    )
    role_arn = response.role.arn

    policy_arns.each do |policy_arn|
      @iam_client.attach_role_policy(
        role_name: role_name,
        policy_arn: policy_arn
      )
    end

    role_arn
  rescue Aws::IAM::Errors::ServiceError => e
    @logger.error("Error creating role: #{e.message}")
    nil
  end
```

- Para obter detalhes da API, consulte CreateRolea Referência AWS SDK for Ruby da API.

Rust

SDK para Rust

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
```

```
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- Para obter detalhes da API, consulte a CreateRolereferência da API AWS SDK for Rust.

Swift

SDK para Swift

> **Note**
>
> Esta é a documentação de pré-lançamento de um SDK na versão de visualização. Está sujeita a alteração.

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
    public func createRole(name: String, policyDocument: String) async throws ->
String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
```

```
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            throw error
        }
    }
```

- Para obter detalhes da API, consulte CreateRolea referência da API AWS SDK for Swift.

Começando AWS Config com o AWS CLI

> **Note**
>
> Antes de configurar AWS Config com o AWS CLI, você precisa criar um bucket do S3, um tópico do SNS e uma função do IAM com políticas anexadas como pré-requisitos. Em seguida, você pode usar o AWS CLI para especificar o bucket, o tópico e a função do AWS Config. Para configurar seus pré-requisitos, consulte Pré-requisitos AWS Config.

Para começar AWS Config com o AWS CLI, use os comandos put-configuration-recorder, put-delivery-channel e start-configuration-recorder, da seguinte forma:

- O comando `put-configuration-recorder` cria um novo gravador de configuração para registrar as configurações de recursos especificadas.
- O comando `put-delivery-channel` cria um objeto de canal de entrega para fornecer informações de configuração a um bucket do S3 e a um tópico do SNS.
- Depois que um canal de entrega é criado, o `start-configuration-recorder` começa a registrar as configurações de recursos selecionadas, que você pode consultar na sua conta da AWS .

> **Note**
>
> Você pode ter somente um gravador de configuração e um canal de entrega para cada região da AWS em sua conta.

Você pode especificar o nome do gravador e o Amazon Resource Name (ARN) da função do IAM assumida e usada AWS Config pelo gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração. Não é possível alterar o nome do gravador de configuração depois de ele ser criado. Para alterar o nome do gravador de configuração, você deverá excluí-lo e criar um novo gravador de configuração com um novo nome.

AWS Config Para configurar a agregação de dados multirregionais de várias contas com o AWS CLI, consulte Configurando um agregador usando a AWS interface de linha de comando. Você deve criar um gravador de configuração separado para cada região em cada uma na Conta da AWS qual deseja registrar os itens de configuração.

Sumário

- put-configuration-recorder
- put-delivery-channel
- start-configuration-recorder

put-configuration-recorder

O comando `put-configuration-recorder` deve se parecer com o exemplo seguinte.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Esse comando usa `--configuration-recorder` os `---recording-group` campos e.

> **Note**
>
> Grupo de gravação e gravador de configuração
>
> O campo `--recording-group` especifica quais tipos de recursos são gravados.
>
> O `--configuration-recorder` campo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é

possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

Grupo de gravação

O `put-configuration-recorder` usa as seguintes opções para o parâmetro `--recording-group`:

- `allSupported=true`— AWS Config registra as alterações na configuração de todos os tipos de recursos compatíveis, excluindo os tipos globais de recursos do IAM. Quando AWS Config adiciona suporte para um novo tipo de recurso, inicia AWS Config automaticamente a gravação de recursos desse tipo.
- `includeGlobalResourceTypes=true`: essa opção é um pacote que se aplica apenas aos tipos globais de recursos do IAM: usuários, grupos, perfis e políticas gerenciadas pelo cliente do IAM. Esses tipos de recursos globais do IAM só podem ser registrados AWS Config em regiões onde AWS Config estavam disponíveis antes de fevereiro de 2022. Você não pode registrar os tipos de recursos globais do IAM nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

> **Important**
>
> Os clusters globais do Aurora são gravados em todas as regiões habilitadas
> O tipo de `AWS::RDS::GlobalCluster` recurso será registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado, mesmo se `includeGlobalResourceTypes` estiver definido como. `false` A opção `includeGlobalResourceTypes` é um pacote que se aplica apenas a usuários, grupos e perfis do IAM, além de políticas gerenciadas pelo cliente.
> Se você não quiser registrar `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, use uma das seguintes estratégias de registro:
>
> 1. Registrar todos os tipos de recursos atuais e futuros com exclusões (`EXCLUSION_BY_RESOURCE_TYPES`)
> 2. Registrar tipos de recursos específicos (`INCLUSION_BY_RESOURCE_TYPES`)
>
> Para obter mais informações, consulte Selecting Which Resources are Recorded.

> **Important**
>
> inclusão GlobalResourceTypes e a estratégia de registro de exclusão
>
> O `includeGlobalResourceTypes` campo não tem impacto na estratégia `EXCLUSION_BY_RESOURCE_TYPES` de gravação. Isso significa que os tipos globais de recursos do IAM (usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM) não serão adicionados automaticamente como exclusões de `exclusionByResourceTypes` quando `includeGlobalResourceTypes` estiver definido como. `false`
>
> O `includeGlobalResourceTypes` campo só deve ser usado para modificar o `AllSupported` campo, pois o padrão para o `AllSupported` campo é registrar as alterações de configuração para todos os tipos de recursos compatíveis, exceto os tipos de recursos globais do IAM. Para incluir os tipos de recursos globais do IAM quando `AllSupported` estiver definido como`true`, certifique-se de `includeGlobalResourceTypes` definir como`true`.
>
> Para excluir os tipos de recursos globais do IAM para a estratégia de `EXCLUSION_BY_RESOURCE_TYPES` gravação, você precisa adicioná-los manualmente ao `resourceTypes` campo de`exclusionByResourceTypes`.

> **Note**
>
> Campos obrigatórios e opcionais
>
> Para definir `includeGlobalResourceTypes` como `true`, defina o campo `allSupported` como `true`.
>
> Também há a opção de definir o campo `useOnly` de `RecordingStrategy` como `ALL_SUPPORTED_RESOURCE_TYPES`.

> **Note**
>
> Campos de substituição
>
> Se você `includeGlobalResourceTypes` definir como`false`, mas listar os tipos globais de recursos do IAM no `resourceTypes` campo de RecordingGroup, ainda AWS Config registrará as alterações de configuração para esses tipos de recursos especificados,

independentemente de você definir o `includeGlobalResourceTypes` campo como false.
Se você não quiser gravar as alterações na configuração dos tipos globais de recursos do IAM (usuários, grupos e perfis do IAM e políticas gerenciadas pelo cliente), não as liste no campo `resourceTypes`, além de definir o campo `includeGlobalResourceTypes` como falso.

- `recordingStrategy`: especifica a estratégia de registro para o gravador de configuração. O arquivo `recordingGroup.json` especifica que tipos de recursos o AWS Config registrará:
  - Se você definir o `useOnly` campo de RecordingStrategyparaALL_SUPPORTED_RESOURCE_TYPES, AWS Config registrará as alterações de configuração para todos os tipos de recursos compatíveis, excluindo os tipos de recursos globais do IAM. Opcionalmente, você pode definir o `allSupported` campo de RecordingGroupparatrue. Quando AWS Config adiciona suporte para um novo tipo de recurso, inicia AWS Config automaticamente a gravação de recursos desse tipo.
  - Se você definir o `useOnly` campo de RecordingStrategycomoINCLUSION_BY_RESOURCE_TYPES, AWS Config registrará as alterações de configuração somente para os tipos de recursos especificados no `resourceTypes` campo de RecordingGroup.
  - Se você definir o `useOnly` campo de RecordingStrategyparaEXCLUSION_BY_RESOURCE_TYPES, AWS Config registra as alterações de configuração para todos os tipos de recursos suportados, exceto os tipos de recursos que você especifica para excluir do registro no `resourceTypes` campo de ExclusionByResourceTypes.

> **Note**
>
> Campos obrigatórios e opcionais
> O campo `recordingStrategy` é opcional quando você define o campo `allSupported` de `--recording-group` para `true`.
> O campo `recordingStrategy` é opcional quando você lista os tipos de recursos no campo `resourceTypes` de `--recording-group`.
> O campo `recordingStrategy` é obrigatório se você listar os tipos de recursos a serem excluídos do registro no campo `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Campos de substituição
>
> Se você escolher `EXCLUSION_BY_RESOURCE_TYPES` para a estratégia de gravação, o campo `exclusionByResourceTypes` substituirá outras propriedades na solicitação. Por exemplo, mesmo que você defina `includeGlobalResourceTypes` como falso, os tipos globais de recursos do IAM gravados globalmente serão automaticamente gravados nessa opção, a menos que esses tipos de recursos sejam especificamente listados como exceções no campo `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Tipos de recursos globais e a estratégia de gravação de exclusão de recursos
>
> Por padrão, se você escolher a estratégia de `EXCLUSION_BY_RESOURCE_TYPES` gravação, quando AWS Config adiciona suporte para um novo tipo de recurso na região em que você configurou o gravador de configuração, incluindo tipos de recursos globais, AWS Config começa a gravar recursos desse tipo automaticamente.
>
> A menos que seja especificamente listado como exclusões, `AWS::RDS::GlobalCluster` será gravado automaticamente em todas as AWS Config regiões suportadas onde o gravador de configuração estiver ativado.
>
> Usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM serão registrados na região em que você configurou o gravador de configuração, se essa for uma região em que AWS Config estava disponível antes de fevereiro de 2022. Você não pode registrar os tipos de recursos globais do IAM nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

O exemplo a seguir mostra a sintaxe de solicitação do `recordingGroup.json`.

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
```

```
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

> **Note**
>
> Políticas de autorização para evitar AWS Organizations acessos
>
> Se você usa uma função preexistente do IAM, verifique se não há uma política de autorização AWS Organizations que impeça a permissão AWS Config de registrar seus recursos. Para obter mais informações sobre políticas de autorização para AWS Organizations, consulte Gerenciamento de políticas AWS Organizations no Guia AWS Organizations do usuário.
>
> Mantenha as permissões mínimas ao reutilizar uma função do IAM
>
> Se você usa um AWS serviço que usa AWS Config, como AWS Security Hub ou AWS Control Tower, e uma função do IAM já foi criada, certifique-se de que a função do IAM que você usa durante a configuração AWS Config mantenha as mesmas permissões mínimas da função preexistente do IAM. Você deve fazer isso para garantir que o outro AWS serviço continue funcionando conforme o esperado.
>
> Por exemplo, se AWS Control Tower tiver uma função do IAM que AWS Config permite ler objetos do S3, certifique-se de que as mesmas permissões sejam concedidas à função do IAM que você usa ao configurar AWS Config. Caso contrário, isso pode interferir na forma como AWS Control Tower opera.

> **Note**
>
> Alto número de AWS Config avaliações
>
> Você pode notar um aumento na atividade em sua conta durante a gravação do mês inicial com o AWS Config em comparação com os meses subsequentes. Durante o processo inicial de inicialização, AWS Config executa avaliações em todos os recursos da sua conta que você selecionou para serem registrados. AWS Config
>
> Se você estiver executando cargas de trabalho efêmeras, poderá observar um aumento na atividade ao registrar AWS Config as alterações de configuração associadas à criação e exclusão desses recursos temporários. Um workload efêmero é um uso temporário

de recursos de computação que são carregados e executados quando necessário. Os exemplos incluem instâncias spot do Amazon Elastic Compute Cloud (Amazon EC2), trabalhos do Amazon EMR e. AWS Auto Scaling Se quiser evitar o aumento da atividade decorrente da execução de cargas de trabalho efêmeras, você pode configurar o gravador de configuração para excluir esses tipos de recursos do registro ou executar esses tipos de cargas de trabalho em uma conta separada, AWS Config desativada, para evitar maiores registros de configuração e avaliações de regras.

> **Note**
>
> Disponibilidade de regiões
>
> Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você está AWS Config configurando. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões com suporte AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você está configurando AWS Config.

Gravador de configuração do

O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--configuration-recorder`:

- `name`— O nome do gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração.
- `roleARN`— Amazon Resource Name (ARN) da função do IAM assumida AWS Config e usada pelo gravador de configuração.
- `recordingMode`— Especifica a frequência de gravação padrão AWS Config usada para registrar as alterações na configuração. AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.

- `recordingFrequency`— A frequência de gravação padrão AWS Config usada para registrar alterações na configuração.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- `recordingModeOverrides`: esse campo permite especificar as substituições para o modo de gravação. É uma matriz de objetos `recordingModeOverride`. Cada objeto `recordingModeOverride` na matriz `recordingModeOverrides` consiste em três campos:
  - `description`: uma descrição fornecida para a substituição.
  - `recordingFrequency`: a frequência de gravação que será aplicada a todos os tipos de recursos especificados na substituição.
  - `resourceTypes`— Uma lista separada por vírgulas que especifica quais tipos de recursos AWS Config estão incluídos na substituição.

> **Note**
>
> Campos obrigatórios e opcionais
>
> O campo `recordingMode` para `put-configuration-recorder` é opcional. Por padrão, a frequência de gravação do gravador de configuração é definida como gravação contínua.

> **Note**
>
> Limites
>
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Para a estratégia de gravação Registrar todos os tipos de recursos compatíveis atuais e futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), esses tipos de recursos serão definidos como Gravação contínua.

O `configurationRecorder.json` arquivo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

put-delivery-channel

Os exemplos de códigos a seguir mostram como usar `PutDeliveryChannel`.

CLI

AWS CLI

Para criar um canal de entrega

O comando a seguir fornece as configurações do canal de entrega como código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

O `deliveryChannel.json` arquivo especifica os atributos do canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Esse exemplo define os seguintes atributos:

`name`- O nome do canal de entrega. Por padrão, o AWS Config atribui o nome `default` a um novo canal de entrega. Você não pode atualizar o nome do canal de entrega com o comando. `put-delivery-channel` Para ver as etapas para alterar o nome, consulte Renomear o canal de entrega. `s3BucketName` - O nome do bucket do Amazon S3 para o qual o AWS Config entrega snapshots de configuração e arquivos de histórico de configuração. Se você especificar um bucket que pertença a outra AWS conta, esse bucket deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para buckets do Amazon S3.

`snsTopicARN`- O Amazon Resource Name (ARN) do tópico do Amazon SNS para o qual o AWS Config envia notificações sobre alterações na configuração. Se você escolher um tópico de outra conta, o tópico deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para o tópico do Amazon SNS.

`configSnapshotDeliveryProperties`- Contém o `deliveryFrequency` atributo, que define com que frequência o AWS Config fornece instantâneos de configuração e com que frequência ele invoca avaliações para regras periódicas do Config.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar as configurações do seu canal de entrega, execute o describe-delivery-channels comando.

- Para obter detalhes da API, consulte PutDeliveryChannel in AWS CLI Command Reference.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo altera a propriedade deliveryFrequency de um canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Para obter detalhes da API, consulte PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

start-configuration-recorder

Para finalizar a ativação AWS Config, use o `start-configuration-recorder`comando.

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Verificando se foi AWS Config iniciado com sucesso com o AWS CLI

Depois de iniciar AWS Config, você pode usar AWS CLI comandos para verificar se o AWS Config está em execução e se AWS Config criou um gravador de configuração e um canal de entrega. Você também pode confirmar que AWS Config começou a gravar e fornecer configurações para o canal de entrega.

Sumário

- Verificar se o canal de entrega foi criado
- Verificar se o gravador de configuração foi criado
- Verifique se a gravação AWS Config foi iniciada

Verificar se o canal de entrega foi criado

Use o comando `describe-delivery-channels` para verificar se o seu bucket do Amazon S3 e o tópico do Amazon SNS foram configurados.

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

Quando você usa a CLI, a API de serviço ou os SDKs para configurar seu canal de entrega e não especifica um nome, atribui AWS Config automaticamente o nome "". `default`

Verificar se o gravador de configuração foi criado

Use o comando `describe-configuration-recorders` para verificar se um gravador de configuração foi criado e se ele assumiu um perfil do IAM. Para ter mais informações, consulte Criar um perfil do IAM.

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

Verifique se a gravação AWS Config foi iniciada

Use o `describe-configuration-recorder-status`comando para verificar se AWS Config ele começou a registrar as configurações dos AWS recursos suportados existentes em sua conta. As configurações registradas são entregues no canal de entrega especificado.

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
```

```
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

O valor `true`, no campo `recording`, confirma que o gravador de configuração começou a registrar as configurações de todos os seus recursos. O AWS Config registra o horário em UTC. A saída é exibida como um timestamp Unix.

Para obter informações sobre a pesquisa de recursos existentes em sua conta e entender as configurações de seus recursos, consulte Exibir histórico e configurações de recursos da .

Usando AWS Config com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.

Documentação do SDK	Exemplos de código
AWS SDK for C++	AWS SDK for C++ exemplos de código
AWS CLI	AWS CLI exemplos de código
AWS SDK for Go	AWS SDK for Go exemplos de código
AWS SDK for Java	AWS SDK for Java exemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript exemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin exemplos de código
AWS SDK for .NET	AWS SDK for .NET exemplos de código
AWS SDK for PHP	AWS SDK for PHP exemplos de código

Documentação do SDK	Exemplos de código
AWS Tools for PowerShell	Ferramentas para exemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) exemplos de código
AWS SDK for Ruby	AWS SDK for Ruby exemplos de código
AWS SDK para Rust	AWS SDK para Rust exemplos de código
SDK da AWS para SAP ABAP	SDK da AWS para SAP ABAP exemplos de código
AWS SDK for Swift	AWS SDK for Swift exemplos de código

Exemplo de disponibilidade

Você não consegue encontrar o que precisa? Solicite um código de exemplo no link Fornecer feedback na parte inferior desta página.

Gerenciar o gravador de configurações

AWS Config usa o gravador de configuração para detectar alterações em suas configurações de recursos e capturar essas alterações como itens de configuração. Você deve criar um gravador de configuração antes de AWS Config poder rastrear suas configurações de recursos. Quando você inicia o gravador de configuração, AWS Config faz um inventário de todos os AWS recursos da sua conta.

Você pode ter somente um canal de gravador de configuração por AWS região Conta da AWS, e é necessário usar AWS Config o canal de entrega.

Se você configurar AWS Config usando o console ou a AWS CLI, cria e inicia AWS Config automaticamente o gravador de configuração para você. Para ter mais informações, consulte Começando com AWS Config.

Por padrão, o gravador de configuração registra todos os recursos com suporte na região em que o AWS Config está em execução. Você pode criar um gravador de configuração personalizado que registra apenas os tipos de recursos que você especificar. Para ter mais informações, consulte AWS Recursos de gravação.

Você paga taxas de uso do serviço quando AWS Config inicia a gravação das configurações. Para obter informações sobre a definição de preço, consulte Definição de preço do AWS Config.

> **Important**
>
> Os resultados da avaliação de recursos excluídos poderão ser mantidos se o gravador de configuração estiver desligado
> Se o gravador de configuração estiver desligado, ele desativará a capacidade de AWS Config rastrear alterações na configuração de seus recursos, incluindo suas exclusões. Isso significa que será possível ver os resultados da avaliação de recursos excluídos anteriormente se você desativar o gravador de configuração.

Gerenciar o gravador de configurações (Console)

Você pode usar o AWS Config console para parar ou iniciar o gravador de configuração. Também é possível alterar a frequência de gravação do gravador de configuração.

To stop or start the configuration recorder

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configurações no painel de navegação.
3. Parar ou iniciar o gravador de configuração:
   - Se você deseja interromper o registro, em Recording is on (O registro está ativo), escolha Turn off (Desativar). Quando solicitado, escolha Continuar.
   - Se você desejar iniciar o registro, em Recording is off (O registro está desativado), escolha Turn on (Ativar). Quando solicitado, escolha Continuar.

To change the recording frequency

AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado. Para obter mais informações, consulte Frequência de gravação.

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configurações no painel de navegação.
3. Selecione Editar para ver as opções em “Frequência de gravação”.

Gerenciar o gravador de configurações (AWS CLI)

Você pode usar o AWS CLI para parar ou iniciar o gravador de configuração. Você também pode renomear ou excluir o gravador de configuração usando a AWS CLI AWS Config API ou um dos AWS SDKs. As etapas a seguir o ajudam a usar o AWS CLI.

To stop the configuration recorder

Use o comando `stop-configuration-recorder`:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

To start the configuration recorder

Use o comando `start-configuration-recorder`:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

To change the recording frequency

Use o comando `put-configuration-recorder` para alterar a frequência de gravação do gravador de configuração:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

O `configurationRecorder.json` arquivo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--configuration-recorder`:

- `name`— O nome do gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração.

- `roleARN`— Amazon Resource Name (ARN) da função do IAM assumida AWS Config e usada pelo gravador de configuração.
- `recordingMode`— Especifica a frequência de gravação padrão AWS Config usada para registrar as alterações de configuração. AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.
  - `recordingFrequency`— A frequência de gravação padrão AWS Config usada para registrar alterações na configuração.

    > **Note**
    >
    > AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

  - `recordingModeOverrides`: esse campo permite especificar as substituições para o modo de gravação. É uma matriz de objetos `recordingModeOverride`. Cada objeto `recordingModeOverride` na matriz `recordingModeOverrides` consiste em três campos:
    - `description`: uma descrição fornecida para a substituição.
    - `recordingFrequency`: a frequência de gravação que será aplicada a todos os tipos de recursos especificados na substituição.
    - `resourceTypes`— Uma lista separada por vírgulas que especifica quais tipos de recursos AWS Config estão incluídos na substituição.

> **Note**
>
> Campos obrigatórios e opcionais
> O campo `recordingMode` para `put-configuration-recorder` é opcional. Por padrão, a frequência de gravação do gravador de configuração é definida como gravação contínua.

> **Note**
>
> Limites
>
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Para a estratégia de gravação Registrar todos os tipos de recursos compatíveis atuais e futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), esses tipos de recursos serão definidos como Gravação contínua.

To delete the configuration recorder

Use o comando `delete-configuration-recorder`:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

To rename the configuration recorder

Para alterar o nome do gravador de configuração, você deverá excluí-lo e criar um novo gravador de configuração com o nome desejado.

1. Use o comando `describe-configuration-recorders` para pesquisar o nome do seu gravador de configuração atual:

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. Use o comando `delete-configuration-recorder` para excluir o gravador de configuração atual:

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

3. Use o comando `put-configuration-recorder` para criar um gravador de configuração com o nome desejado:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. Use o comando `start-configuration-recorder` para retomar a gravação:

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

Detecção de desvio para o gravador de configuração

O tipo de recursos `AWS::Config::ConfigurationRecorder` é um item de configuração (CI) para o gravador de configuração que rastreia todas as alterações no estado do gravador de configuração. Você pode usar esse CI para verificar se o estado do gravador de configuração é diferente ou se desviou do estado anterior. Por exemplo, esse CI rastreia se há atualizações nos tipos de recursos que você habilitou AWS Config para rastrear, se você interrompeu ou iniciou o gravador de configuração ou se excluiu ou desinstalou o gravador de configuração. Um gravador de configuração desviada indica que você não está detectando com precisão as alterações nos tipos de recursos pretendidos. Se o gravador de configuração tiver sido desviado, isso pode resultar em resultados de conformidade falsos negativos ou falsos positivos.

O tipo de `AWS::Config::ConfigurationRecorder` recurso é um tipo de recurso do sistema AWS Config e o registro desse tipo de recurso é ativado por padrão em todas as regiões suportadas. A gravação para o tipo de recurso `AWS::Config::ConfigurationRecorder` vem sem custo adicional.

Gerenciar o canal de entrega

Ao registrar AWS Config continuamente as alterações que ocorrem em seus AWS recursos, ele envia notificações e estados de configuração atualizados por meio do canal de entrega. Você pode gerenciar o canal de entrega para controlar para onde AWS Config envia as atualizações de configuração.

Você pode ter apenas um canal de entrega por AWS região por região Conta da AWS, e é necessário usar o canal de entrega AWS Config.

Quando AWS Config detecta uma alteração na configuração de um recurso e a notificação excede o tamanho máximo permitido pelo Amazon SNS, a notificação inclui um breve resumo do item de configuração. Você pode visualizar a notificação completa no local do bucket do S3 especificado no campo `s3BucketLocation`. Para obter mais informações, consulte Example Oversized Configuration Item Change Notification.

> **Note**
>
> AWS Config oferece suporte à AWS KMS criptografia para buckets Amazon S3 usados pelo AWS Config
>
> Você pode fornecer uma chave AWS Key Management Service (AWS KMS) ou um alias Amazon Resource Name (ARN) para criptografar os dados entregues ao seu bucket do Amazon Simple Storage Service (Amazon S3). Por padrão, AWS Config entrega histórico de configuração e arquivos de snapshot ao seu bucket Amazon S3 e criptografa os dados em repouso usando a criptografia do lado do servidor S3 AES-256, SSE-S3. No entanto, se você AWS Config fornecer sua chave KMS ou o alias ARN, AWS Config use essa chave KMS em vez da criptografia AES-256.
>
> AWS Config não suporta o canal de entrega para um bucket do Amazon S3 em que o bloqueio de objetos está habilitado com a retenção padrão ativada. Para obter mais informações, consulte Como o bloqueio de objetos do S3 funciona.

Tópicos

- Terminologia
- Atualizar o canal de entrega
- Renomear o canal de entrega
- Componentes de um item de configuração

- Entregando snapshots de configuração para um bucket do Amazon S3
- Notificações que o AWS Config envia para um tópico do Amazon SNS

Terminologia

Um item de configuração representa uma point-in-time visualização dos vários atributos de um AWS recurso compatível que existe em sua conta. Os componentes de um item de configuração incluem metadados, atributos, relacionamentos, configuração atual e eventos relacionados. AWS Config cria um item de configuração sempre que detecta uma alteração em um tipo de recurso que está gravando. Por exemplo, se AWS Config estiver gravando buckets do Amazon S3, AWS Config cria um item de configuração sempre que um bucket é criado, atualizado ou excluído. Você também pode selecionar AWS Config para criar um item de configuração na frequência de gravação que você definiu.

Histórico de configuração é uma coleção de itens de configuração para um recurso específico durante um período. Um histórico de configuração pode ajudar a responder perguntas sobre, por exemplo, quando o recurso foi criado, como o recurso foi configurado no decorrer do último mês, e que alterações de configuração foram feitas ontem, às 9h. O histórico de configuração está disponível para você em vários formatos. AWS Config entrega automaticamente um arquivo de histórico de configuração para cada tipo de recurso que está sendo gravado em um bucket do Amazon S3 que você especificar. Você pode selecionar um determinado recurso no AWS Config console e navegar até todos os itens de configuração anteriores desse recurso usando a linha do tempo. Além disso, você pode acessar o histórico de itens de configuração para um recurso a partir da API.

Snapshot de configuração é uma coleção de itens de configuração dos recursos compatíveis existentes na conta. Esse snapshot de configuração é uma imagem completa dos recursos que estão sendo registrados e suas configurações. O snapshot de configuração pode ser uma ferramenta útil para validar sua configuração. Por exemplo, talvez você queira examinar o snapshot de configuração regularmente para recursos que são configurados incorretamente ou que potencialmente não devem existir. O snapshot de configuração está disponível em vários formatos. O snapshot de configuração pode ser enviado a um bucket do Amazon Simple Storage Service (Amazon S3) que você especificar. Além disso, você pode selecionar um momento no AWS Config console e navegar pelo instantâneo dos itens de configuração usando as relações entre os recursos.

Um fluxo de configuração é uma lista atualizada automaticamente de todos os itens de configuração dos recursos que estão AWS Config sendo gravados. Toda vez que um recurso é criado,

modificados ou excluídos, o AWS Config cria um item de configuração e o adiciona ao stream de configuração. O fluxo de configuração funciona usando um tópico do Amazon Simple Notification Service (Amazon SNS) de sua escolha. O fluxo de configuração é útil para observar as alterações de configuração à medida que elas ocorrem, para que você possa identificar possíveis problemas, gerar notificações se determinados recursos forem alterados ou atualizar sistemas externos que precisam refletir a configuração de seus AWS recursos.

Atualizar o canal de entrega

Ao atualizar o canal de entrega, você pode definir as seguintes opções:

- O bucket do Amazon S3 para o qual AWS Config envia instantâneos de configuração e arquivos de histórico de configuração.
- Com que frequência AWS Config entrega snapshots de configuração para seu bucket do Amazon S3.
- O tópico do Amazon SNS para o qual AWS Config envia notificações sobre alterações na configuração.

Para atualizar o canal de entrega (Console)

Você pode usar o AWS Config console para definir o bucket do Amazon S3 e o tópico do Amazon SNS para seu canal de entrega. Sobre as etapas para gerenciar essas configurações, consulte Configurando AWS Config com o console.

O console não fornece opções para renomear o canal de entrega, definir a frequência para a configuração de snapshots ou excluir o canal de entrega. Para realizar essas tarefas, você deve usar a AWS CLI AWS Config API ou um dos AWS SDKs.

Para atualizar o canal de entrega (AWS SDKs)

Os exemplos de códigos a seguir mostram como usar `PutDeliveryChannel`.

CLI

AWS CLI

Para criar um canal de entrega

O comando a seguir fornece as configurações do canal de entrega como código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

O `deliveryChannel.json` arquivo especifica os atributos do canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Esse exemplo define os seguintes atributos:

`name`- O nome do canal de entrega. Por padrão, o AWS Config atribui o nome `default` a um novo canal de entrega. Você não pode atualizar o nome do canal de entrega com o comando. `put-delivery-channel` Para ver as etapas para alterar o nome, consulte Renomear o canal de entrega. `s3BucketName` - O nome do bucket do Amazon S3 para o qual o AWS Config entrega snapshots de configuração e arquivos de histórico de configuração. Se você especificar um bucket que pertença a outra AWS conta, esse bucket deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para buckets do Amazon S3.

`snsTopicARN`- O Amazon Resource Name (ARN) do tópico do Amazon SNS para o qual o AWS Config envia notificações sobre alterações na configuração. Se você escolher um tópico de outra conta, o tópico deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para o tópico do Amazon SNS.

`configSnapshotDeliveryProperties`- Contém o `deliveryFrequency` atributo, que define com que frequência o AWS Config fornece instantâneos de configuração e com que frequência ele invoca avaliações para regras periódicas do Config.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar as configurações do seu canal de entrega, execute o describe-delivery-channels comando.

- Para obter detalhes da API, consulte PutDeliveryChannel in AWS CLI Command Reference.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo altera a propriedade deliveryFrequency de um canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Para obter detalhes da API, consulte PutDeliveryChannel in AWS Tools for PowerShell Cmdlet Reference.

(Opcional) Você pode usar o comando `describe-delivery-channels` para verificar se as configurações de canal de entrega estão atualizadas:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

Os exemplos de códigos a seguir mostram como usar `DescribeDeliveryChannels`.

CLI

AWS CLI

Para obter detalhes sobre o canal de entrega

O comando a seguir retorna detalhes sobre o canal de entrega:

```
aws configservice describe-delivery-channels
```

Saída:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeDeliveryCanais na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo recupera o canal de entrega da região e exibe detalhes.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Saída:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obter detalhes da API, consulte DescribeDeliveryChannels in AWS Tools for PowerShell Cmdlet Reference.

Renomear o canal de entrega

Para alterar o nome do canal de entrega, você deve excluí-lo e criar um novo canal de entrega com o nome desejado. Antes de excluir o canal de entrega, você deve interromper temporariamente o gravador de configuração.

O AWS Config console não oferece a opção de excluir o canal de entrega, então você deve usar a AWS CLI, a AWS Config API ou um dos AWS SDKs.

Para renomear o canal de entrega (AWS CLI)

Renomeando o canal de entrega usando o AWS CLI

1. Use o comando `stop-configuration-recorder` para interromper o gravador de configuração:

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. Use o comando `describe-delivery-channels` e anote os atributos de seu canal de entrega:

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. Use o comando `delete-delivery-channel` para excluir o canal de entrega:

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. Use o comando `put-delivery-channel` para criar um canal de entrega com o nome desejado:

```
$ aws configservice put-delivery-channel --delivery-channel file:// deliveryChannel.json
```

O arquivo deliveryChannel.json especifica os atributos do canal de entrega:

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. Use o comando `start-configuration-recorder` para retomar a gravação:

```
$ aws configservice start-configuration-recorder --configuration-recorder-name configRecorderName
```

Componentes de um item de configuração

Um item de configuração representa uma point-in-time visualização dos vários atributos de um AWS recurso compatível que existe em sua conta. Os componentes de um item de configuração incluem metadados, atributos, relacionamentos, configuração atual e eventos relacionados. AWS Config cria um item de configuração sempre que detecta uma alteração em um tipo de recurso que está gravando. Por exemplo, se AWS Config estiver gravando buckets do Amazon S3, AWS Config cria um item de configuração sempre que um bucket é criado, atualizado ou excluído. Você também pode selecionar AWS Config para criar um item de configuração na frequência de gravação que você definiu.

Um item de configuração é composto dos seguintes componentes.

Componente	Descrição	Contém
Metadados	As informações sobre este item de configuração	• ID da versão • Horário em que o item de configuração foi capturado • Status do item de configuração, indicando se o item foi capturado com êxito • ID do estado indicando a ordem dos itens de configuração de um recurso
Atributos	Atributos de recursos	• ID do recurso • Lista de tags de valores-chave para esse recurso • Tipo de recurso (consulte Tipos de recursos compatíveis) • Nome do recurso da Amazon (ARN) • Zona de disponibilidade que contém esse recurso, se aplicável • Hora em que o recurso foi criado
Relacionamentos	Como o recurso é relacionado a outros recursos associados com a conta	Descrição do relacionamento, como o volume `vol-1234567` do Amazon EBS é vinculado a uma instância `i-a1b2c3d4` do Amazon EC2
Configuração atual	Informações retornadas por meio de uma chamada para a API Describe ou List do recurso	Por exemplo, a API `DescribeVolumes` retorna as seguintes informações sobre o volume: • Zona de disponibilidade em que o volume está • Hora em que o volume foi vinculado • ID da instância EC2 a que o volume está vinculado • Status atual do volume

Componente	Descrição	Contém
		• Estado da DeleteOnTermination bandeira • Dispositivo ao qual o volume está vinculado • Tipo de volume, como `gp2`, `io1`, ou `standard`

Observações

1. Um item de configuração de relacionamento não inclui dependências de fluxo de dados ou de fluxo de rede. Os itens de configuração não podem ser personalizados para representar sua arquitetura de aplicativo.
2. Da versão 1.3 em diante, o campo relatedEvents está vazio. Você pode acessar a LookupEvents API na Referência da AWS CloudTrail API para recuperar os eventos do recurso.
3. Da versão 1.3 em diante, o campo configurationItemMD5Hash está vazio. Você pode usar o configurationStateId campo para garantir que você tenha o item de configuração mais recente.

Entregando snapshots de configuração para um bucket do Amazon S3

AWS Config fornece instantâneos de configuração dos AWS recursos que estão AWS Config sendo gravados no bucket do Amazon S3 que você especificou ao configurar seu canal de entrega.

Tópicos

- Entregando instantâneos de configuração
- Exemplo de instantâneo de configuração de AWS Config
- Verificar o status de entrega
- Visualizar o snapshot de configuração no bucket do Amazon S3

Entregando instantâneos de configuração

AWS Config gera instantâneos de configuração quando você invoca a ação DeliverConfigSnapshot ou executa o comando. AWS CLI `deliver-config-snapshot` AWS Config armazena snapshots de configuração no bucket do Amazon S3 que você especificou quando habilitou. AWS Config

Digite o `deliver-config-snapshot`comando especificando o nome atribuído por AWS Config quando você configurou seu canal de entrega, por exemplo:

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

Exemplo de instantâneo de configuração de AWS Config

Veja a seguir um exemplo das informações AWS Config incluídas em um instantâneo de configuração. O snapshot descreve a configuração dos recursos que você AWS Config Conta da AWS está gravando na região atual e descreve as relações entre esses recursos.

> **Note**
>
> O snapshot de configuração pode incluir referências a tipos de recursos e IDs de recursos que não têm suporte.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
```

```
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
```

```
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
```

```
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
```

```
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
```

```
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

A próxima etapa é verificar se o snapshot de configuração foi entregue com êxito para o canal de entrega.

Verificar o status de entrega

Digite o `describe-delivery-channel-status`comando para verificar se o AWS Config começou a entregar as configurações para o canal de entrega especificado, por exemplo:

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
```

```
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

A resposta lista o status de todos os três formatos de entrega AWS Config usados para fornecer configurações para seu bucket e tópico.

Veja o campo `lastSuccessfulTime` em `configSnapshotDeliveryInfo`. O horário deve corresponder ao momento em que você solicitou a entrega do snapshot de configuração.

> **Note**
>
> AWS Config usa o formato UTC (Tempo Universal Coordenado) para registrar a hora.

Visualizar o snapshot de configuração no bucket do Amazon S3

1. Faça login no AWS Management Console e abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
2. Na lista Todos os buckets do console do Amazon S3, clique no nome do bucket do Amazon S3.
3. Clique nas pastas aninhadas em seu bucket até ver o objeto `ConfigSnapshot` com um ID de snapshot correspondente ao ID retornado pelo comando. Faça o download e abra o objeto para visualizar o snapshot de configuração.

   O bucket do S3 também contém um arquivo vazio chamado`ConfigWritabilityCheckFile`. AWS Config cria esse arquivo para verificar se o serviço pode gravar com êxito no bucket do S3.

Notificações que o AWS Config envia para um tópico do Amazon SNS

> **Note**
>
> Antes de AWS Config poder enviar notificações para um tópico do Amazon SNS, você deve primeiro configurar o gravador de configuração e o canal de entrega. Para obter mais informações, consulte Gerenciando o gravador de configuração e Gerenciando o canal de entrega.

Você pode configurar o AWS Config para transmitir as alterações de configuração e notificações para um tópico do Amazon SNS. Por exemplo, quando um recurso é atualizado, você pode receber uma notificação em seu e-mail, para que possa visualizar as alterações. Você também pode ser notificado quando o AWS Config avaliar suas regras gerenciadas ou personalizadas em relação aos seus recursos. Para obter mais informações, consulte Logging and Monitoring in AWS Config.

O AWS Config envia notificações sobre os seguintes eventos:

- Alteração de item de configuração de um recurso.
- Histórico de configuração de um recurso entregue para a sua conta.
- Snapshot de configuração para recursos registrados iniciado e entregue para a sua conta.
- Estado de compatibilidade de seus recursos e se são compatíveis com suas regras.
- Avaliação iniciada para uma regra em relação a seus recursos.
- O AWS Config falhou ao entregar a notificação para sua conta.

Tópicos

- Exemplos de notificações de alteração de item de configuração
- Exemplo de notificação de entrega de histórico de configuração
- Exemplo de notificação de entrega de snapshot de configuração iniciada
- Exemplo de notificação de entrega de snapshot de configuração
- Exemplo de notificação de alteração de compatibilidade
- Exemplo de notificação de avaliação de regras iniciada
- Exemplo de notificação de alteração de item de configuração superdimensionado

- Exemplo de notificação de falha na entrega

Exemplos de notificações de alteração de item de configuração

AWS Config usa o Amazon SNS para entregar notificações aos endpoints de assinatura. Essas notificações fornecem o status de entrega de instantâneos e históricos de configuração e fornecem cada item de configuração AWS Config criado quando as configurações dos recursos registrados AWS são alteradas. AWS Config também envia notificações que mostram se seus recursos estão em conformidade com suas regras. Se optar por receber as notificações por e-mail, você pode usar filtros no seu aplicativo cliente de e-mail com base na linha de assunto e no corpo da mensagem de e-mail.

Veja a seguir apresentamos um exemplo de carga de uma notificação do Amazon SNS que é gerada quando o AWS Config detecta que o volume `vol-ce676ccc` do Amazon Elastic Block Store está vinculado à instância com um ID de `i-344c463d`. A notificação contém a alteração do item de configuração para o recurso.

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
```

```
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::INSTANCE",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [],
                "volumeType": "standard"
            }
        }
    ],
    "configurationItemDiff": {
        "changeType": "UPDATE",
        "changedProperties": {
            "Configuration.State": {
                "previousValue": "available",
                "updatedValue": "in-use",
                "changeType": "UPDATE"
            },
            "Configuration.Attachments.0": {
                "updatedValue": {
                    "VolumeId": "vol-ce676ccc",
                    "InstanceId": "i-344c463d",
                    "Device": "/dev/sdf",
                    "State": "attached",
                    "AttachTime": "FriMar0723: 46: 28UTC2014",
                    "DeleteOnTermination": "false"
                },
```

```
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```

Itens de configuração para recursos com relacionamentos

Se um recurso está relacionado com outros recursos, uma alteração nesse recurso pode resultar em vários itens de configuração. O exemplo a seguir mostra como AWS Config cria itens de configuração para recursos com relacionamentos.

1. Você tem uma instância do Amazon EC2 com o ID de `i-007d374c8912e3e90` e a instância está associada a um grupo de segurança do Amazon EC2, `sg-c8b141b4`.
2. Você atualiza sua instância EC2 para alterar o grupo de segurança para outro grupo de segurança, `sg-3f1fef43`.
3. Como a instância do EC2 está relacionada a outro recurso, AWS Config cria vários itens de configuração, como os exemplos a seguir:

Essa notificação contém a alteração do item de configuração para a instância EC2 quando o grupo de segurança é substituído.

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
```

```
   "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
in Account 123456789012",
   "Message": {
       "configurationItemDiff": {
           "changedProperties": {
               "Configuration.NetworkInterfaces.0": {
                   "previousValue": {
                       "networkInterfaceId": "eni-fde9493f",
                       "subnetId": "subnet-2372be7b",
                       "vpcId": "vpc-14400670",
                       "description": "",
                       "ownerId": "123456789012",
                       "status": "in-use",
                       "macAddress": "0e:36:a2:2d:c5:e0",
                       "privateIpAddress": "172.31.16.84",
                       "privateDnsName": "ip-172-31-16-84.ec2.internal",
                       "sourceDestCheck": true,
                       "groups": [{
                           "groupName": "example-security-group-1",
                           "groupId": "sg-c8b141b4"
                       }],
                       "attachment": {
                           "attachmentId": "eni-attach-85bd89d9",
                           "deviceIndex": 0,
                           "status": "attached",
                           "attachTime": "2017-01-09T19:36:02.000Z",
                           "deleteOnTermination": true
                       },
                       "association": {
                           "publicIp": "54.175.43.43",
                           "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                           "ipOwnerId": "amazon"
                       },
                       "privateIpAddresses": [{
                           "privateIpAddress": "172.31.16.84",
                           "privateDnsName": "ip-172-31-16-84.ec2.internal",
                           "primary": true,
                           "association": {
                               "publicIp": "54.175.43.43",
                               "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                               "ipOwnerId": "amazon"
                           }
```

```
                }]
            },
            "updatedValue": null,
            "changeType": "DELETE"
        },
        "Relationships.0": {
            "previousValue": {
                "resourceId": "sg-c8b141b4",
                "resourceName": null,
                "resourceType": "AWS::EC2::SecurityGroup",
                "name": "Is associated with SecurityGroup"
            },
            "updatedValue": null,
            "changeType": "DELETE"
        },
        "Configuration.NetworkInterfaces.1": {
            "previousValue": null,
            "updatedValue": {
                "networkInterfaceId": "eni-fde9493f",
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "description": "",
                "ownerId": "123456789012",
                "status": "in-use",
                "macAddress": "0e:36:a2:2d:c5:e0",
                "privateIpAddress": "172.31.16.84",
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "sourceDestCheck": true,
                "groups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "attachment": {
                    "attachmentId": "eni-attach-85bd89d9",
                    "deviceIndex": 0,
                    "status": "attached",
                    "attachTime": "2017-01-09T19:36:02.000Z",
                    "deleteOnTermination": true
                },
                "association": {
                    "publicIp": "54.175.43.43",
                    "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                    "ipOwnerId": "amazon"
```

```
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
```

```
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                "stateTransitionReason": "",
```

```
                "keyName": "ec2-micro",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t2.micro",
                "launchTime": "2017-01-09T20:13:28.000Z",
                "placement": {
                    "availabilityZone": "us-east-2c",
                    "groupName": "",
                    "tenancy": "default",
                    "hostId": null,
                    "affinity": null
                },
                "kernelId": null,
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
```

```
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
```

```
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Essa notificação contém a alteração do item de configuração para o grupo de segurança EC2, `sg-3f1fef43`, que está associado com a instância.


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
```

```
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
```

```
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Noções básicas sobre o campo **`configurationItemDiff`** nas notificações **`ConfigurationItemChangeNotification`** do Amazon SNS

AWS Config cria um item de configuração sempre que a configuração de um recurso é alterada (criar/atualizar/excluir). Para obter uma lista dos tipos de recursos compatíveis que AWS Config podem gravar, consulteTipos de recursos compatíveis. AWS Config usa o Amazon SNS para enviar uma notificação à medida que as alterações ocorrem. A carga de notificação do Amazon SNS inclui campos para ajudar você a rastrear as alterações de recursos em uma determinada região. AWS

Para entender por que você recebe uma notificação `ConfigurationItemChangeNotification`, revise os detalhes de `configurationItemDiff`. Os campos variam de acordo com o tipo de alteração e podem formar combinações diferentes, como UPDATE-UPDATE, UPDATE-CREATE e DELETE-DELETE. A seguir estão explicações de algumas combinações comuns.

UPDATE-CREATE e UPDATE-UPDATE

O exemplo a seguir inclui alterações nas relações diretas de recursos e nas configurações de recursos. Os detalhes de `configurationItemDiff` revelam as seguintes informações:

Ação realizada: uma política gerenciada presente na conta foi anexada a uma função AWS Identity and Access Management (IAM).

Operação básica executada: UPDATE (atualização do número de associações do tipo de recurso do `AWS::IAM::Policy` em uma conta).

Alterar combinações de tipos:

1. Alteração direta do relacionamento com o recurso UPDATE-CREATE. Um novo anexo ou associação foi criado entre uma política do IAM e um perfil do IAM.
2. Alteração na configuração do recurso UPDATE-UPDATE. O número de associações de políticas do IAM aumentou de dois para três quando a política foi anexada ao perfil do IAM.

Exemplo de notificação de `configurationItemDiff` UPDATE-CREATE e UPDATE-UPDATE:

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                 >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                 >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

O exemplo a seguir inclui alterações nas relações diretas de recursos e nas configurações de recursos. Os detalhes de `configurationItemDiff` revelam as seguintes informações:

Ação executada: uma política gerenciada presente na conta foi separada de um usuário do IAM.

Operação básica executada: UPDATE (atualização da política de permissões associada ao tipo de recurso `AWS::IAM::User`).

Combinações de tipo de alteração: alteração do relacionamento direto do recurso UPDATE-DELETE. A associação entre um usuário do IAM e uma política do IAM em uma conta foi excluída.

Exemplo de notificação de `configurationItemDiff` UPDATE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
```

```
  }
}
```

DELETE-DELETE

O exemplo a seguir inclui alterações nas relações diretas de recursos e nas configurações de recursos. Os detalhes de `configurationItemDiff` revelam as seguintes informações:

Ação realizada: um perfil do IAM presente em uma conta foi excluído.

Operação básica executada: DELETE (um recurso do tipo de recurso do `AWS::IAM::Role` foi excluído).

Combinações de tipos de alteração: alteração do relacionamento direto do recurso e alteração da configuração do recurso DELETE-DELETE. A exclusão do perfil do IAM também excluiu a associação da política do IAM com o perfil do IAM.

Exemplo de notificação de `configurationItemDiff` DELETE-DELETE:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
```

```
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

Exemplo de notificação de entrega de histórico de configuração

O histórico de configuração é uma coleção de itens de configuração para um tipo de recurso durante um período de tempo. Veja a seguir um exemplo de notificação que é AWS Config enviada quando o histórico de configuração de um recurso de CloudTrail trilha é entregue à sua conta.

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
```

```
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemplo de notificação de entrega de snapshot de configuração iniciada

O exemplo a seguir é de uma notificação que o AWS Config envia quandoAWS Configinicia a entrega de um snapshot de configuração para a sua conta.


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Exemplo de notificação de entrega de snapshot de configuração

O snapshot de configuração é uma coleção de itens de configuração para todos os recursos registrados e suas configurações em sua conta. O exemplo a seguir é de uma notificação que o AWS Config envia quando o snapshot de configuração é entregue para a sua conta.


```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb
+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/
TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemplo de notificação de alteração de compatibilidade

Quando o AWS Config avalia seus recursos em relação a uma regra gerenciada ou personalizada, AWS Configele envia uma notificação que mostra se os recursos são compatíveis com a regra.

Veja a seguir um exemplo de notificação em que o recurso de CloudTrail trilha está em conformidade com a regra `cloudtrail-enabled` gerenciada.


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
```

```
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


Exemplo: alteração do item de configuração do Config | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
```

```
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
```

```
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

Exemplo de notificação de avaliação de regras iniciada

O AWS Config envia uma notificação quando ele inicia a avaliação de sua regra gerenciada ou personalizada em relação a seus recursos. O exemplo a seguir é de uma notificação de quando o AWS Config inicia a avaliação da regra gerenciada `iam-password-policy`.

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
```

```
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

Exemplo de notificação de alteração de item de configuração superdimensionado

Quando o AWS Config detecta uma alteração de configuração de um recurso, ele envia uma notificação de item de configuração. Se a notificação exceder o tamanho máximo permitido pelo Amazon Simple Notification Service (Amazon SNS), a notificação incluirá um breve resumo do item de configuração. Você pode visualizar a notificação completa na localização do bucket do Amazon S3 especificada no `s3BucketLocation` campo.

O exemplo de notificação a seguir mostra um item de configuração para uma instância do Amazon EC2. A notificação inclui um resumo das alterações e a localização da notificação no bucket do Amazon S3.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.

    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
```

```
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

Exemplo de notificação de falha na entrega

AWS Configenvia uma notificação de falha na entrega se não AWS Config conseguir entregar o snapshot de configuração ou uma notificação de alteração de item de configuração de tamanho grande para seu bucket do Amazon S3. Verifique se você especificou um bucket válido do Amazon S3.

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the
 maximum size allowed by Amazon Simple Notification Service (SNS). A summary of the
 configuration item is provided here. You can view the complete notification in the
 specified Amazon S3 bucket location.
```

```
    New State Record Summary:
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

Gerenciando e visualizando configurações AWS de recursos com AWS Config

AWS Config permite avaliar, auditar e avaliar as configurações dos AWS recursos.

AWS recursos são entidades que você cria e gerencia usando o AWS Management Console, a AWS Command Line Interface (CLI), os AWS SDKs ou AWS as ferramentas de parceiros. Exemplos de AWS recursos incluem instâncias do Amazon EC2, grupos de segurança, Amazon VPCs e Amazon Elastic Block Store. AWS Config refere-se a cada recurso usando seu identificador exclusivo, como o ID do recurso ou um nome de recurso da Amazon (ARN).

Alguns casos de uso comuns incluem:

- Administrador de nuvem: você pode rastrear e gerenciar configurações de recursos para ajudar a garantir a conformidade, solucionar problemas e manter uma compreensão do seu ambiente AWS
- Analista de segurança: você pode avaliar as configurações de recursos em relação aos estados desejados para ajudar a identificar vulnerabilidades e avaliar a postura de segurança.
- Diretor de conformidade: você pode auditar e monitorar continuamente as configurações dos recursos para ajudar a garantir a adesão às políticas organizacionais e aos padrões do setor.

Tópicos

- Visualizando o AWS Config painel
- Tipos de recursos compatíveis
- Cobertura de recursos por região e disponibilidade
- AWS Recursos de gravação
- Configurações de registro para recursos de terceiros
- Registrar a configuração de software para instâncias gerenciadas
- Exibir histórico e configurações de recursos da
- Marcar os recursos do AWS Config

Visualizando o AWS Config painel

Use o painel para ter uma visão geral de seus recursos, regras, pacotes de conformidade e seus estados de conformidade e para visualizar suas métricas de AWS Config uso e sucesso com a

Amazon. CloudWatch Esta página ajuda você a identificar rapidamente os principais recursos em sua AWS conta, os pacotes de conformidade com o nível mais baixo de conformidade Conta da AWS, quais regras ou recursos não estão em conformidade com sua Conta da AWS, qual tráfego está impulsionando seu AWS Config uso e as principais métricas de sucesso e fracasso que ocorreram em seus fluxos de trabalho.

Para usar o AWS Config painel

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No painel de navegação à esquerda, escolha Painel.

Sumário

- Inventário de conformidade e recursos
- AWS Config Métricas de uso e sucesso

Inventário de conformidade e recursos

Após a configuração, AWS Config começa a registrar os recursos especificados e a avaliá-los de acordo com suas regras. Pode levar alguns minutos AWS Config para exibir seus recursos, regras, pacotes de conformidade e seus estados de conformidade.

Pacotes de conformidade por pontuação de conformidade

Os pacotes de conformidade por pontuação de conformidade exibem até 10 dos seus pacotes de conformidade com a pontuação de conformidade mais baixa. A pontuação de conformidade é a porcentagem do número de combinações de recursos e regras compatíveis em um pacote de conformidade em comparação com o número total de combinações possíveis de regras e recursos.

Essa métrica fornece uma visão de alto nível do estado de conformidade de seus pacotes de conformidade e pode ser usada para identificar, investigar e entender o nível de conformidade em seus pacotes de conformidade. Você pode usar a pontuação de conformidade para monitorar o progresso da correção, realizar comparações entre diferentes conjuntos de requisitos e ver o impacto que uma mudança ou implantação específica tem em um pacote de conformidade.

Para ver o status da implantação, a pontuação de conformidade, o cronograma da pontuação de conformidade e as regras de um pacote de conformidade em uma exibição detalhada, escolha o nome do pacote de conformidade em Pacote de conformidade.

Compliance status (Status de conformidade)

O Status de conformidade exibe o número de suas regras e recursos compatíveis e não compatíveis. Os recursos estão em conformidade ou não com base em uma avaliação da regra associada a eles. Se um recurso não seguir as especificações da regra, o recurso e a regra serão marcados como não compatíveis.

Para ver a lista de regras e recursos incompatíveis, escolha Regras incompatíveis ou Recursos incompatíveis.

Regras de recursos incompatíveis

Regras por recursos incompatíveis exibe suas principais regras incompatíveis em ordem decrescente pelo número de recursos. Escolha uma regra para ver seus detalhes, parâmetros e os recursos no escopo dessa regra específica.

Para obter uma lista abrangente de regras incompatíveis, escolha Visualizar todas as regras não compatíveis.

Inventário de recursos

O inventário de recursos exibe o número total de recursos que AWS Config está sendo registrado em ordem decrescente pelo número de recursos e a contagem de cada tipo de recurso no seu Conta da AWS. Para abrir todos os recursos de um tipo de recurso, escolha esse tipo de recurso para acessar sua página Inventário de recursos.

Você pode usar a lista suspensa para indicar quais totais de recursos você deseja visualizar. Por padrão, ele está configurado para exibir Todos os recursos, mas você pode alterá-lo para AWS recursos, recursos de terceiros ou recursos personalizados.

> **Note**
>
> A mensagem Avalie sua configuração de AWS recursos usando regras de configuração pode aparecer no Painel pelos seguintes motivos:
>
> - Você não configurou AWS Config regras para o seu Conta da AWS. Você pode escolher Add rule (Adicionar regra) para ir para a página Rules (Regras).

- AWS Config ainda está avaliando seus recursos de acordo com suas regras. Você pode atualizar a página para ver os resultados de avaliação mais recentes.
- AWS Config avaliou seus recursos de acordo com suas regras e não encontrou nenhum recurso no escopo. Você pode especificar os recursos AWS Config para gravar na página Configurações. Para ter mais informações, consulte AWS Recursos de gravação.

AWS Config Métricas de uso e sucesso

Você pode usar os CloudWatch painéis da Amazon no AWS Config console para visualizar suas métricas de AWS Config uso e sucesso.

Para cada painel, você pode fazer o seguinte:

- Ajuste o intervalo de tempo do painel para exibir dados das últimas 3 horas, 1 dia ou 1 semana.
- Escolha o ícone Calendário para inserir um intervalo de tempo personalizado: um tempo relativo para um período especificado anterior ou um intervalo de tempo absoluto entre duas datas.
- Você pode alterar o formato da hora para exibir os dados do painel em UTC (Hora Universal Coordenada) ou fuso horário local (o fuso horário especificado como seu fuso horário local no sistema operacional do seu dispositivo).
- Use a Seta suspensa ao lado do ícone Atualizar para especificar com que frequência os dados em um painel devem ser atualizados ou para desabilitar a atualização automática. Escolha Desativado, dez segundos, um minuto, dois minutos, cinco minutos ou 15 minutos.
- Escolha Mais opções (o menu de reticências verticais) para adicionar as métricas de AWS Config uso ou as métricas de AWS Config sucesso que você está visualizando atualmente no AWS Config Painel ao console. CloudWatch Isso abre uma nova guia no CloudWatch console que permite criar um novo painel personalizado CloudWatch com informações copiadas de suas métricas de AWS Config uso ou métricas de AWS Config sucesso atuais.

Se você quiser realizar análises adicionais dessas métricas com CloudWatch, escolha Métricas no painel de navegação esquerdo do CloudWatch console e escolha AWS/Config. Para obter mais informações sobre o que você pode fazer no CloudWatch console, consulte Usando CloudWatch painéis da Amazon e Usando CloudWatch métricas da Amazon no Guia do CloudWatch usuário.

AWS Config Métricas de uso

Métrica	Descrição	Unidade	
`Configuration Items Recorded`	O número de itens de configuração registrados para cada tipo de recurso ou todos os tipos de recursos. Um item de configuração representa uma point-in-time visão dos vários atributos de um AWS recurso suportado. Para obter mais informações sobre itens de configuração ou tipos de recursos compatíveis, consulte Itens de configuração e Tipos de recursos compatíveis.	Contagem	

Você pode selecionar o tipo de recurso que deseja visualizar usando a lista suspensa. Por padrão, ela está configurada para exibir todos os tipos de recursos.

AWS Config Métricas de sucesso

Métrica	Descrição	Unidade	
`Change Notifications Delivery Failed`	O número de entregas malsucedidas de notificação de alteração para o tópico do Amazon SNS para seu canal de entrega. Uma notificação de alteração informa sobre uma alteração no estado da configuração dos seus AWS recursos. Você pode usar a ConfigStreamDeliveryInfoAPI para obter a notificação de alteração `lastErrorCode` ou `lastErrorMessage` para a última tentativa de entrega. Para obter mais informações, consulte Gerenciar o canal de entrega.	Contagem	
`Config History`	O número de exportações do histórico de configuração com falha para seu bucket do Amazon S3. Um histórico de configura	Contagem	

Métrica	Descrição	Unidade	
`Export Failed`	ção é uma coleção de itens de configura ção para determinado recurso durante um período. Para obter mais informações sobre o histórico de configurações, consulte Histórico de configurações.		
`Configuration Recorder Insufficient Permissions Failure`	O número de tentativas malsucedidas de acesso à permissão devido à política de função do IAM para o gravador de configura ção ter permissões insuficientes. Usa o gravador de configurações para detectar alterações nas configurações do seu recurso e capturar as alterações como itens de configuração. Para que o gravador de configuração registre suas configurações AWS de recursos, ele requer as permissõe s necessárias do IAM. Para obter mais informações, consulte IAM Role Policy for Getting Configuration Details.	Contagem	
`Config Snapshot Export Failed`	O número de exportações de snapshots de configuração com falha para seu bucket do Amazon S3. Um snapshot de configuração é uma coleção de itens de configuração para os recursos compatíveis existentes em sua conta. Para obter mais informações sobre esses snapshots de configuração, consulte Snapshot de configuração.	Contagem	

Tipos de recursos compatíveis

> **Important**
>
> Esta página é atualizada mensalmente no início de cada mês.

AWS Config suporta os seguintes tipos de AWS recursos e relacionamentos de recursos.

- Para obter informações mais detalhadas sobre um tipo de recurso, consulte suas informações de referência (como sintaxe, propriedades e valores de retorno) na referência de tipos de AWS recursos e propriedades no Guia do AWS CloudFormation usuário.
- Para AWS Config gravação, algumas AWS regiões oferecem suporte a um subconjunto desses tipos de recursos. Para obter informações sobre quais tipos de recursos são compatíveis em quais regiões, consulte Disponibilidade de recursos por região.
- As consultas avançadas oferecem AWS Config suporte a um subconjunto desses tipos de recursos. Para obter uma lista de tipos de recursos compatíveis, consulte Supported Resource Types for Advanced Queries.
- A avaliação proativa AWS Config oferece suporte a um subconjunto desses tipos de recursos. Para obter uma lista desses tipos de recursos compatíveis, consulte Supported Resource Types for Proactive Evaluation.
- As regras periódicas são executadas sem que o gravador de configuração esteja habilitado, pois elas não dependem dos itens de configuração. Para obter mais informações sobre a diferença entre regras acionadas por alterações e regras periódicas, consulte Modo de avaliação e tipos de gatilho para regras. AWS Config

> **Note**
>
> Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você AWS Config configurou. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você configurou AWS Config.

Amazon AppStream

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	N/D	N/D
	`AWS::AppStream::Application`	N/D	N/D
	`AWS::AppStream::Stack`	N/D	N/D
	`AWS::AppStream::Fleet`	N/D	N/D

Amazon AppFlow

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon AppFlow	`AWS::AppFlow::Flow`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon AppIntegrations	`AWS::AppIntegrations::EventIntegration`	N/D	N/D

Amazon API Gateway

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
API Gateway	`AWS::ApiGateway::Stage`	está contido em	ApiGateway API Rest
		está associado a	WebACL do WAFRegional
	`AWS::ApiGateway::RestApi`	contém	ApiGateway Palco
API Gateway V2	`AWS::ApiGatewayV2::Stage`	está contido em	ApiGatewayAPI V2
	`AWS::ApiGatewayV2::Api`	contém	ApiGatewayEstágio V2

Para saber mais sobre como AWS Config se integra ao Amazon API Gateway, consulte Monitorando a configuração da API Gateway com AWS Config.

Amazon Athena

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Athena	`AWS::Athena::WorkGroup`	N/D	N/D
	`AWS::Athena::DataCatalog`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Athena::PreparedStatement`	N/D	N/D

Amazon CloudFront

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon CloudFront	`AWS::CloudFront::Distribution`	está associado a	AWS WebACL WAF
			Certificado do ACM
			S3 Bucket
			Certificado de servidor do IAM
	`AWS::CloudFront::StreamingDistribution`	está associado a	AWS WebACL WAF
			Certificado do ACM
			S3 Bucket
			Certificado de servidor do IAM

Amazon CloudWatch

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	N/D	N/D
	`AWS::CloudWatch::MetricStream`	N/D	N/D
CloudWatch Registros da Amazon	`AWS::Logs::Destination`	N/D	N/D
Amazon CloudWatch RUM	`AWS::RUM::AppMonitor`	N/D	N/D
Amazon, CloudWatch evidentemente	`AWS::Evidently::Project`	N/D	N/D
	`AWS::Evidently::Launch`	N/D	N/D
	`AWS::Evidently::Segment`	N/D	N/D

Amazon CodeGuru

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
CodeGuru Revisor da Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	N/D	N/D

Amazon Cognito

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Cognito	`AWS::Cognito::UserPool`	N/D	N/D
	`AWS::Cognito::UserPoolClient`	N/D	N/D
	`AWS::Cognito::UserPoolGroup`	N/D	N/D

Amazon Connect

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Connect	`AWS::Connect::PhoneNumber`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Connect::QuickConnect`	N/D	N/D
	`AWS::Connect::Instance`	N/D	N/D
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	N/D	N/D
	`AWS::CustomerProfiles::ObjectType`	N/D	N/D

Amazon Detective

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Detective	`AWS::Detective::Graph`	N/D	N/D

Amazon DynamoDB

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon DynamoDB	`AWS::DynamoDB::Table`	N/D	N/D

Amazon Elastic Compute Cloud

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Elastic Compute Cloud	`AWS::EC2::Host` *	contém	EC2 instance (Instância do EC2)
	`AWS::EC2::EIP`	é anexado a	EC2 instance (Instância do EC2)
			Interface de rede
	`AWS::EC2::Instance`	contém	Interface de rede EC2
		está associado a	Security group EC2
		é anexado a	Volume do Amazon EBS
			IP elástico EC2 (EIP)
		está contido em	Host dedicado EC2
			Tabela de rotas
			Sub-rede
			Nuvem privada virtual (VPC)
	`AWS::EC2::NetworkInterface`	está associado a	Security group EC2
		é anexado a	IP elástico EC2 (EIP)
			EC2 instance (Instância do EC2)
		está contido em	Tabela de rotas
			Sub-rede

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Nuvem privada virtual (VPC)
	`AWS::EC2::SecurityGroup` *	está associado a	EC2 instance (Instância do EC2)
			Interface de rede EC2
			Nuvem privada virtual (VPC)
	`AWS::EC2::NatGateway`	está contido em	Virtual private cloud (VPC)
		está contido em	Sub-rede
	`AWS::EC2::EgressOnlyInternetGateway`	é anexado a	Nuvem privada virtual (VPC)
	`AWS::EC2::EC2Fleet`	N/D	N/D
	`AWS::EC2::SpotFleet`	N/D	N/D
	`AWS::EC2::PrefixList`	N/D	N/D
	`AWS::EC2::FlowLog`	N/D	N/D
	`AWS::EC2::TransitGateway`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::EC2::TransitGatewayAttachment`	N/D	N/D
	`AWS::EC2::TransitGatewayRouteTable`	N/D	N/D
	`AWS::EC2::VPCEndpoint`	está contido em	Virtual private cloud (VPC)
		é anexado a	Interface de rede
		está contido em	Sub-rede
		está contido em	Tabela de rotas
	`AWS::EC2::VPCEndpointService`	está associado a	ElasticLoadBalancamento V2 LoadBalancer
	`AWS::EC2::VPCPeeringConnection`	está associado a	Nuvem privada virtual (VPC)
	`AWS::EC2::RegisteredHAInstance`	está associado a	EC2 instance (Instância do EC2)
	`AWS::EC2::SubnetRouteTableAssociation`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::EC2::LaunchTemplate`	N/D	N/D
	`AWS::EC2::NetworkInsightsAccessScopeAnalysis`	N/D	N/D
	`AWS::EC2::TrafficMirrorTarget`	N/D	N/D
	`AWS::EC2::TrafficMirrorSession`	N/D	N/D
	`AWS::EC2::DHCPOptions`	N/D	N/D
	`AWS::EC2::IPAM`	N/D	N/D
	`AWS::EC2::NetworkInsightsPath`	N/D	N/D
	`AWS::EC2::TrafficMirrorFilter`	N/D	N/D
	`AWS::EC2::CapacityReservation`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::EC2::ClientVpnEndpoint`	N/D	N/D
	`AWS::EC2::CustomerGateway`	é anexado a	VPN connection (Conexão VPN)
	`AWS::EC2::InternetGateway`	é anexado a	Nuvem privada virtual (VPC)
	`AWS::EC2::NetworkAcl`	N/D	N/D
	`AWS::EC2::RouteTable`	contém	EC2 instance (Instância do EC2)
			Interface de rede EC2
			Sub-rede
			gateway VPN
		está contido em	Virtual private cloud (VPC)
	`AWS::EC2::Subnet`	contém	EC2 instance (Instância do EC2)
			Interface de rede EC2
		é anexado a	Conexão ACL
		está contido em	Tabela de rotas

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Nuvem privada virtual (VPC)
	`AWS::EC2::VPC`	contém	EC2 instance (Instância do EC2)
			Interface de rede EC2
			Conexão ACL
			Tabela de rotas
			Sub-rede
		está associado a	Grupo de segurança
	`AWS::EC2::VPNConnection`	é anexado a	Gateway da Internet
			gateway VPN
		é anexado a	Gateway do cliente
			gateway VPN
	`AWS::EC2::VPNGateway`	é anexado a	Nuvem privada virtual (VPC)
			VPN connection (Conexão VPN)
		está contido em	Tabela de rotas
	`AWS::EC2::IPAMScope`	N/D	N/D
	`AWS::EC2::CarrierGateway`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::EC2::TransitGatewayConnect`	N/D	N/D
	`AWS::EC2::IPAMPool`	N/D	N/D
	`AWS::EC2::TransitGatewayMulticastDomain`	N/D	N/D
	`AWS::EC2::NetworkInsightsAccessScope`	N/D	N/D
	`AWS::EC2::NetworkInsightsAnalysis`	N/D	N/D
Amazon Elastic Block Store	`AWS::EC2::Volume`	é anexado a	EC2 instance (Instância do EC2)
EC2 Image Builder	`AWS::ImageBuilder::ImagePipeline`	N/D	N/D
	`AWS::ImageBuilder::DistributionConfiguration`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::ImageBuilder::ContainerRecipe`	N/D	N/D
	`AWS::ImageBuilder::InfrastructureConfiguration`	N/D	N/D
	`AWS::ImageBuilder::ImageRecipe`	N/D	N/D

*AWS Config registra os detalhes de configuração dos hosts dedicados e as instâncias que você executa neles. Como resultado, você pode usar AWS Config como fonte de dados ao relatar a conformidade com suas licenças de software vinculadas ao servidor. Por exemplo, você pode visualizar o histórico de configuração de uma instância e determinar em que Imagem de máquina da Amazon (AMI) ele é baseado. Em seguida, você pode examinar o histórico de configuração do host, que inclui detalhes como o número de soquetes e núcleos, para verificar se o host é compatível com os requisitos de licença da AMI. Para obter mais informações, consulte Rastreando alterações de configuração AWS Config no Guia do usuário do Amazon EC2.

* A definição de SecurityGroup propriedades do EC2 contém blocos IP CIDR, que são convertidos em intervalos de IP internamente e podem retornar resultados inesperados ao tentar encontrar um intervalo IP específico. Para soluções alternativas para pesquisar intervalos de IP específicos, consulte Limitations for Advanced Queries.

Amazon Elastic Container Registry

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Elastic Container Registry	`AWS::ECR::Repository`	N/D	N/D
	`AWS::ECR::RegistryPolicy`	N/D	N/D
	`AWS::ECR::PullThroughCacheRule`	N/D	N/D
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	N/D	N/D

Amazon Elastic Container Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Elastic Container Service	`AWS::ECS::Cluster`	N/D	N/D
	`AWS::ECS::TaskDefinition`	N/D	N/D
	`AWS::ECS::Service` *	N/D	N/D
	`AWS::ECS::TaskSet`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::ECS::Capacity Provider`	N/D	N/D

*Atualmente, esse serviço é compatível apenas com o novo formato de nome do recurso da Amazon (ARN). Para obter mais informações, consulte Nomes de recursos da Amazon (ARNs) e IDs no guia do desenvolvedor do ECS.

Antigo (não compatível): `arn:aws:ecs:region:aws_account_id:service/service-name`

Novo (compatível): `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Elastic File System	`AWS::EFS::FileSystem`	N/D	N/D
	`AWS::EFS::AccessPoint`	N/D	N/D

Amazon Elastic Kubernetes Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::EKS::FargateProfile`	N/D	N/D
	`AWS::EKS::IdentityProviderConfig`	N/D	N/D
	`AWS::EKS::Addon`	N/D	N/D

Amazon EMR

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon EMR	`AWS::EMR::SecurityConfiguration`	N/D	N/D

Amazon EventBridge

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon EventBridge	`AWS::Events::EventBus`	N/D	N/D
	`AWS::Events::ApiDestination`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Events::Archive`	N/D	N/D
	`AWS::Events::Endpoint`	N/D	N/D
	`AWS::Events::Connection`	N/D	N/D
	`AWS::Events::Rule`	N/D	N/D
EventBridge Esquemas da Amazon	`AWS::EventSchemas::RegistryPolicy`	N/D	N/D
	`AWS::EventSchemas::Discoverer`	N/D	N/D
	`AWS::EventSchemas::Schema`	N/D	N/D

Amazon Forecast

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Forecast	`AWS::Forecast::Dataset`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Forecast::DatasetGroup`	N/D	N/D

Amazon Fraud Detector

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Fraud Detector	`AWS::FraudDetector::Label`	N/D	N/D
	`AWS::FraudDetector::EntityType`	N/D	N/D
	`AWS::FraudDetector::Variable`	N/D	N/D
	`AWS::FraudDetector::Outcome`	N/D	N/D

Amazon GuardDuty

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon GuardDuty	`AWS::GuardDuty::Detector`	N/D	N/D
	`AWS::GuardDuty::ThreatIntelSet`	N/D	N/D
	`AWS::GuardDuty::IPSet`	N/D	N/D
	`AWS::GuardDuty::Filter`	N/D	N/D

Amazon Inspector

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Inspector	`AWS::InspectorV2::Filter`	N/D	N/D

Amazon Interactive Video Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Interactive Video Service	`AWS::IVS::Channel`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::IVS::RecordingConfiguration`	N/D	N/D
	`AWS::IVS::PlaybackKeyPair`	N/D	N/D

Amazon Keyspaces (para Apache Cassandra)

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Keyspaces (para Apache Cassandra)	`AWS::Cassandra::Keyspace`	N/D	N/D

OpenSearch Serviço Amazon

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
OpenSearch Serviço Amazon	`AWS::Elasticsearch::Domain`	está associado a	Chave do KMS
			Security group EC2
			Sub-rede EC2
			Nuvem privada virtual (VPC)
	`AWS::OpenSearch::Domain`	N/D	N/D

> **Note**
>
> Em 8 de setembro de 2021, o Amazon Elasticsearch Service foi renomeado para Amazon Service. OpenSearch OpenSearch Suporte de serviço OpenSearch , bem como OSS legado do Elasticsearch. Para obter mais informações, consulte Amazon OpenSearch Service - Resumo das alterações.
>
> Você pode continuar vendo seus dados `AWS::OpenSearch::Domain` sob o tipo de `AWS::Elasticsearch::Domain` recurso existente por várias semanas, mesmo se atualizar um ou mais domínios para o. OpenSearch

Amazon Personalize

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Personalize	`AWS::Personalize::Dataset`	N/D	N/D
	`AWS::Personalize::Schema`	N/D	N/D
	`AWS::Personalize::Solution`	N/D	N/D
	`AWS::Personalize::DatasetGroup`	N/D	N/D

Amazon Pinpoint

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	N/D	N/D
	`AWS::Pinpoint::Segment`	N/D	N/D
	`AWS::Pinpoint::App`	N/D	N/D
	`AWS::Pinpoint::Campaign`	N/D	N/D
	`AWS::Pinpoint::InAppTemplate`	N/D	N/D
	`AWS::Pinpoint::EmailChannel`	N/D	N/D
	`AWS::Pinpoint::EmailTemplate`	N/D	N/D
	`AWS::Pinpoint::EventStream`	N/D	N/D

Amazon Quantum Ledger Database (Amazon QLDB)

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon QLDB	`AWS::QLDB::Ledger`	N/D	N/D

Amazon Kendra

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Kendra	`AWS::Kendra::Index`	N/D	N/D

Amazon Kinesis

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Kinesis	`AWS::Kinesis::Stream`	N/D	N/D
	`AWS::Kinesis::StreamConsumer`	N/D	N/D
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	N/D	N/D
Amazon Data Firehose	`AWS::KinesisFireho`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`se::DeliveryStream`		
Fluxos de vídeo do Kinesis	`AWS::KinesisVideo::SignalingChannel`	N/D	N/D
	`AWS::KinesisVideo::Stream`	N/D	N/D

Amazon Lex

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Lex	`AWS::Lex::BotAlias`	N/D	N/D
	`AWS::Lex::Bot`	N/D	N/D

Amazon Lightsail

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Lightsail	`AWS::Lightsail::Disk`	N/D	N/D
	`AWS::Lightsail::Certificate`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Lightsail::Bucket`	N/D	N/D
	`AWS::Lightsail::StaticIp`	N/D	N/D

Amazon Lookout for Metrics

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	N/D	N/D

Amazon Lookout for Vision

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	N/D	N/D

Amazon Managed Grafana

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Managed Grafana	`AWS::Grafana::Workspace`	N/D	N/D

Amazon Managed Service para Prometheus

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Managed Service para Prometheus	`AWS::APS::RuleGroupsNamespace`	N/D	N/D

Amazon MemoryDB para Redis

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon MemoryDB para Redis	`AWS::MemoryDB::SubnetGroup`	N/D	N/D

Amazon MQ

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon MQ	`AWS::AmazonMQ::Broker`	N/D	N/D

Amazon Managed Streaming for Apache Kafka

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	N/D	N/D
	`AWS::MSK::Configuration`	N/D	N/D
	`AWS::MSK::BatchScramSecret`	N/D	N/D
	`AWS::MSK::ClusterPolicy`	N/D	N/D
	`AWS::MSK::VpcConnection`	N/D	N/D
Amazon Managed Streaming for Apache Kafka Connect	`AWS::KafkaConnect::Connector`	N/D	N/D

Amazon Redshift

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Redshift	`AWS::Redshift::Cluster`	está associado a	Grupo de parâmetros do cluster
			Security group de cluster

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Grupo de sub-rede de cluster
			Grupo de segurança
			Nuvem privada virtual (VPC)
	`AWS::Redshift::ClusterParameterGroup`	N/D	N/D
	`AWS::Redshift::ClusterSecurityGroup`	N/D	N/D
	`AWS::Redshift::ScheduledAction`	N/D	N/D
	`AWS::Redshift::ClusterSnapshot`	está associado a	Cluster
			Nuvem privada virtual (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	está associado a	Sub-rede
			Nuvem privada virtual (VPC)
	`AWS::Redshift::EventSubscription`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Redshift::EndpointAccess`	N/D	N/D
	`AWS::Redshift::EndpointAuthorization`	N/D	N/D

Amazon Relational Database Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Relational Database Service	`AWS::RDS::DBInstance`	está associado a	Security group EC2
			Grupo de segurança de banco de dados do RDS
			Grupo de sub-rede de banco de dados do RDS
	`AWS::RDS::DBSecurityGroup`	está associado a	Security group EC2
			Nuvem privada virtual (VPC)
	`AWS::RDS::DBSnapshot`	está associado a	Nuvem privada virtual (VPC)
	`AWS::RDS::DBSubnetGroup`	está associado a	Security group EC2

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Nuvem privada virtual (VPC)
	`AWS::RDS::EventSubscription`	N/D	N/D
	`AWS::RDS::DBCluster`	contém	Instância de banco de dados do RDS
		está associado a	Grupo de sub-rede de banco de dados do RDS
			Security group EC2
	`AWS::RDS::DBClusterSnapshot`	está associado a	Cluster de banco de dados do RDS
			Nuvem privada virtual (VPC)
	`AWS::RDS::GlobalCluster`	N/D	N/D
	`AWS::RDS::OptionGroup`	N/D	N/D

Amazon Route 53

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Route 53	`AWS::Route53::HostedZone`	N/D	N/D
	`AWS::Route53::HealthCheck`	N/D	N/D
Amazon Route 53 Resolver	`AWS::Route53Resolver::ResolverEndpoint`	N/D	N/D
	`AWS::Route53Resolver::ResolverRule`	N/D	N/D
	`AWS::Route53Resolver::ResolverRuleAssociation`	N/D	N/D
	`AWS::Route53Resolver::FirewallDomainList`	N/D	N/D
	`AWS::Route53Resolver::FirewallRuleGroupAssociation`	N/D	N/D
	`AWS::Route53Resolver::ResolverQueryLoggingConfig`	N/D	N/D
	`AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation`	N/D	N/D
	`AWS::Route53Resolver::FirewallRuleGroup`	N/D	N/D
Amazon Route 53 Application Recovery Controller	`AWS::Route53RecoveryReadiness::Cell`	N/D	N/D
	`AWS::Route53RecoveryReadiness::ReadinessCheck`	N/D	N/D
	`AWS::Route53RecoveryReadiness::RecoveryGroup`	N/D	N/D
	`AWS::Route53RecoveryControl::Cluster`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Route53RecoveryControl::ControlPanel`	N/D	N/D
	`AWS::Route53RecoveryControl::RoutingControl`	N/D	N/D
	`AWS::Route53RecoveryControl::SafetyRule`	N/D	N/D
	`AWS::Route53RecoveryReadiness::ResourceSet`	N/D	N/D

Amazon SageMaker

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon SageMaker	`AWS::SageMaker::CodeRepository`	N/D	N/D
	`AWS::SageMaker::Domain`	N/D	N/D
	`AWS::SageMaker::AppImageConfig`	N/D	N/D
	`AWS::SageMaker::Image`	N/D	N/D
	`AWS::SageMaker::Model`	N/D	N/D
	`AWS::SageMaker::NotebookInstance`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::SageMaker::NotebookInstanceLifecycleConfig`	N/D	N/D
	`AWS::SageMaker::EndpointConfig`	N/D	N/D
	`AWS::SageMaker::Workteam`	N/D	N/D
	`AWS::SageMaker::FeatureGroup`	N/D	N/D

Amazon Simple Email Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Simple Email Service	`AWS::SES::ConfigurationSet`	N/D	N/D
	`AWS::SES::ContactList`	N/D	N/D
	`AWS::SES::Template`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::SES::ReceiptFilter`	N/D	N/D
	`AWS::SES::ReceiptRuleSet`	N/D	N/D

Amazon Simple Notification Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Simple Notification Service	`AWS::SNS::Topic`	N/D	N/D

Amazon Simple Queue Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Simple Queue Service	`AWS::SQS::Queue`	N/D	N/D

Amazon Simple Storage Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon Simple Storage Service	`AWS::S3::Bucket` *	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::S3::AccountPublicAccessBlock`	N/D	N/D
	`AWS::S3::MultiRegionAccessPoint`	N/D	N/D
	`AWS::S3::StorageLens`	N/D	N/D
	`AWS::S3::AccessPoint`	N/D	N/D

* Se você configurou AWS Config para gravar seus buckets do S3 e não está recebendo notificações de alteração de configuração, verifique se as políticas do bucket do S3 têm as permissões necessárias. Para ter mais informações, consulte Gerenciar permissões para gravação de bucket do S3.

Atributos do bucket do Amazon S3

AWS Config também registra os seguintes atributos para o tipo de recurso de bucket do Amazon S3.

Atributos	Descrição
AccelerateConfiguration	Aceleração para transferência de dados em longas distâncias entre o cliente e um bucket.
BucketAcl	Lista de controle de acesso usada para gerenciar o acesso a buckets e objetos.
BucketPolicy	Política que define as permissões para o bucket.
CrossOriginConfiguração	Permite solicitações de origem cruzada para o bucket.

Atributos	Descrição
LifecycleConfiguration	Regras que definem o ciclo de vida de objetos em seu bucket.
LoggingConfiguration	Registro usado para acompanhar as solicitações de acesso ao bucket.
NotificationConfiguration	Notificações de eventos usadas para enviar alertas ou acionar fluxos de trabalho para eventos do bucket especificado.
ReplicationConfiguration	Cópia assíncrona automática de objetos em buckets, em diferentes regiões AWS .
RequestPaymentConfiguração	Pagamento pelo solicitante está habilitado.
TaggingConfiguration	Tags adicionadas ao bucket para classificar. Você também pode usar tags para acompanhar o faturamento.
WebsiteConfiguration	Hospedagem de site estático está habilitada para o bucket.
VersioningConfiguration	O versionamento está habilitado para objetos no bucket.

Para obter mais informações, sobre os atributos, consulte Opções de configuração do bucket no Guia do usuário do Amazon Simple Storage Service.

Amazon WorkSpaces

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Amazon WorkSpaces	`AWS::WorkSpaces::ConnectionAlias`	N/D	N/D
	`AWS::WorkSpaces::Workspace`	N/D	N/D

AWS Amplify

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Amplify	`AWS::Amplify::App`	N/D	N/D
	`AWS::Amplify::Branch`	N/D	N/D

AWS AppConfig

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS AppConfig	`AWS::AppConfig::Application`	N/D	N/D
	`AWS::AppConfig::Environment`	N/D	N/D
	`AWS::AppConfig::ConfigurationProfile`	N/D	N/D
	`AWS::AppConfig::DeploymentStrategy`	N/D	N/D
	`AWS::AppConfig::HostedConfi`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`gurationVersion`		
	`AWS::AppConfig::ExtensionAssociation`	N/D	N/D

AWS App Runner

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS App Runner	`AWS::AppRunner::VpcConnector`	N/D	N/D
	`AWS::AppRunner::Service`	N/D	N/D

AWS App Mesh

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS App Mesh	`AWS::AppMesh::VirtualNode`	N/D	N/D
	`AWS::AppMesh::VirtualService`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::AppMesh::VirtualGateway`	N/D	N/D
	`AWS::AppMesh::VirtualRouter`	N/D	N/D
	`AWS::AppMesh::Route`	N/D	N/D
	`AWS::AppMesh::GatewayRoute`	N/D	N/D
	`AWS::AppMesh::Mesh`	N/D	N/D

AWS AppSync

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS AppSync	`AWS::AppSync::GraphQLApi`	N/D	N/D

AWS Audit Manager

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Audit Manager	`AWS::AuditManager::Assessment`	N/D	N/D

AWS Auto Scaling

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contém	Instância do Amazon EC2
		está associado a	Classic Load Balancer
			Configuração de execução de Auto Scaling
			Sub-rede
	`AWS::AutoScaling::LaunchConfiguration`	está associado a	Grupo de segurança do Amazon EC2
	`AWS::AutoScaling::ScalingPolicy`	está associado a	Auto Scaling group (Grupo do Auto Scaling)
			Alarme

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::AutoScaling::ScheduledAction`	está associado a	Auto Scaling group (Grupo do Auto Scaling)
	`AWS::AutoScaling::WarmPool`	N/D	N/D

AWS Backup

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Backup	`AWS::Backup::BackupPlan`	N/D	NA*
	`AWS::Backup::BackupSelection`	N/D	N/D
	`AWS::Backup::BackupVault`	N/D	NA*
	`AWS::Backup::RecoveryPoint`	N/D	N/D
	`AWS::Backup::ReportPlan`	N/D	N/D

Devido à forma como AWS Backup funciona, alguns desses tipos de recursos estão relacionados aos outros tipos de AWS Backup recursos desta tabela.

`AWS::Backup::BackupPlan`está relacionado a `AWS::Backup::BackupSelection` onde um Plano de Backup tem muitas opções e `AWS::Backup::BackupVault` está relacionado a `AWS::Backup::RecoveryPoint` onde um AWS Backup Vault tem vários pontos de recuperação.

Para obter mais informações, consulte Managing backups using backup plans e Working with backup vaults.

AWS Batch

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Batch	`AWS::Batch::JobQueue`	N/D	N/D
	`AWS::Batch::ComputeEnvironment`	N/D	N/D
	`AWS::Batch::SchedulingPolicy`	N/D	N/D

AWS Budgets

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Budgets	`AWS::Budgets::BudgetsAction`	N/D	N/D

AWS Certificate Manager

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Certificate Manager	`AWS::ACM::Certificate`	N/D	N/D

AWS CloudFormation

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CloudFormation	`AWS::CloudFormation::Stack` *	contém	Tipos AWS de recursos compatíveis

*AWS Config registra as alterações de configuração nas AWS CloudFormation pilhas e os tipos de recursos suportados nas pilhas. AWS Config não registra alterações de configuração para tipos de recursos na pilha que ainda não são suportados. Os tipos de recursos não compatíveis são exibidos na seção de configurações complementares do item de configuração da pilha.

AWS CloudTrail

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CloudTrail	`AWS::CloudTrail::Trail`	N/D	N/D

AWS Cloud9

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	N/D	N/D

AWS Cloud Map

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Descoberta de serviço	`AWS::ServiceDiscovery::Service`	N/D	N/D
	`AWS::ServiceDiscovery::PublicDnsNamespace`	N/D	N/D
	`AWS::ServiceDiscovery::HttpNamespace`	N/D	N/D
`AWS::ServiceDiscovery::Instance`	N/D	N/D	

AWS CodeArtifact

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	N/D	N/D

AWS CodeBuild

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CodeBuild	`AWS::CodeBuild::Project` *	está associado a	Bucket do S3
			IAM role (Perfil do IAM)
	`AWS::CodeBuild::ReportGroup`	N/D	N/D

* Para saber mais sobre como AWS Config se integra com AWS CodeBuild, consulte Usar AWS Config com AWS CodeBuild amostra.

AWS CodeDeploy

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CodeDeploy	`AWS::CodeDeploy::Application`	contém	DeploymentGroup

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::CodeDeploy::DeploymentConfig`	N/D	N/D
	`AWS::CodeDeploy::DeploymentGroup`	está contido em	Aplicativo

AWS CodePipeline

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS CodePipeline	`AWS::CodePipeline::Pipeline` *	é anexado a	Bucket do S3
		está associado a	IAM role (Perfil do IAM)
			Projeto de código
			Função do Lambda
			Pilha do CloudFormation
			ElasticBeanstalk aplicação

*AWS Config registra as alterações de configuração nos CodePipeline pipelines e os tipos de recursos suportados nos pipelines. AWS Config não registra alterações de configuração para tipos de recursos nos pipelines que ainda não são suportados. Os tipos de recursos não compatíveis, como `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, e `ECS`

`service`, são exibidos na seção de configurações complementares do item de configuração da pilha.

AWS Config

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Config	`AWS::Config::ResourceCompliance` *	está associado a	Todos os recursos *
	`AWS::Config::ConformancePackCompliance`	N/D	N/D
	`AWS::Config::ConfigurationRecorder` *	N/D	N/D

*A relação entre um recurso relacionado à `AWS::Config::ResourceCompliance` e um recurso relacionado depende de como a `AWS::Config::ResourceCompliance` relata a conformidade com esse tipo específico de recurso.

* `AWS::Config::ConfigurationRecorder` é um tipo de recurso do sistema AWS Config e a gravação desse tipo de recurso é ativada por padrão.

> **Note**
>
> A gravação para os tipos de recursos de `AWS::Config::ConformancePackCompliance` e `AWS::Config::ConfigurationRecorder` é fornecida sem custo adicional.

AWS Database Migration Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Database Migration Service	`AWS::DMS::EventSubscription`	N/D	N/D
	`AWS::DMS::ReplicationSubnetGroup`	N/D	N/D
	`AWS::DMS::ReplicationInstance`	N/D	N/D
	`AWS::DMS::ReplicationTask`	N/D	N/D
	`AWS::DMS::Certificate`	N/D	N/D
	`AWS::DMS::Endpoint`	N/D	N/D

AWS DataSync

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS DataSync	`AWS::DataSync::LocationSMB`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::DataSync::LocationFSxLustre`	N/D	N/D
	`AWS::DataSync::LocationFSxWindows`	N/D	N/D
	`AWS::DataSync::LocationS3`	N/D	N/D
	`AWS::DataSync::LocationEFS`	N/D	N/D
	`AWS::DataSync::LocationNFS`	N/D	N/D
	`AWS::DataSync::LocationHDFS`	N/D	N/D
	`AWS::DataSync::LocationObjectStorage`	N/D	N/D
	`AWS::DataSync::Task`	N/D	N/D

AWS Device Farm

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Device Farm	`AWS::DeviceFarm::TestGridProject`	N/D	N/D
	`AWS::DeviceFarm::InstanceProfile`	N/D	N/D
	`AWS::DeviceFarm::Project`	N/D	N/D

AWS Elastic Beanstalk

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Application`	contém	Versão do aplicativo do Elastic Beanstalk
			Ambiente do Elastic Beanstalk
		está associado a	IAM role (Perfil do IAM)
	`AWS::ElasticBeanstalk::ApplicationVersion`	está contido em	Aplicativo do Elastic Beanstalk
		está associado a	Ambiente do Elastic Beanstalk

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Bucket do S3
	`AWS::ElasticBeanstalk::Environment`	está contido em	Aplicativo do Elastic Beanstalk
		está associado a	Versão do aplicativo do Elastic Beanstalk
			IAM role (Perfil do IAM)
		contém	CloudFormation Pilha

AWS Fault Injection Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	N/D	N/D

AWS Global Accelerator

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	N/D	N/D
	`AWS::GlobalAcceler`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`ator::EndpointGroup`		
	`AWS::GlobalAccelerator::Accelerator`	N/D	N/D

AWS Glue

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Glue	`AWS::Glue::Job`	N/D	N/D
	`AWS::Glue::Classifier`	N/D	N/D
	`AWS::Glue::MLTransform`	N/D	N/D

AWS Ground Station

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Ground Station	`AWS::GroundStation::Config`	N/D	N/D
	`AWS::GroundStation`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`::Mission Profile`		
	`AWS::GroundStation::DataflowEndpointGroup`	N/D	N/D

AWS HealthLake

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	N/D	N/D

AWS Identity and Access Management (IAM)

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Identity and Access Management	`AWS::IAM::User`	é anexado a	IAM group (Grupo do IAM)
			Política do IAM gerenciada pelo cliente
	`AWS::IAM::Group`	contém	Usuário do IAM

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
		é anexado a	Política do IAM gerenciada pelo cliente
	`AWS::IAM::Role`	é anexado a	Política do IAM gerenciada pelo cliente
	`AWS::IAM::Policy`	é anexado a	IAM user (Usuário do IAM)
			IAM group (Grupo do IAM)
			IAM role (Perfil do IAM)
	`AWS::IAM::SAMLProvider`	N/D	N/D
	`AWS::IAM::ServerCertificate`	N/D	N/D
	`AWS::IAM::InstanceProfile`	N/D	N/D
	`AWS::IAM::OIDCProvider`	N/D	N/D
AWS Identity and Access Management Access Analyzer	`AWS::AccessAnalyzer::Analyzer`	N/D	N/D

AWS Config inclui políticas em linha com os detalhes de configuração que ele registra. Para obter mais informações sobre políticas em linha, consulte Políticas gerenciadas e em linha no Guia do usuário do IAM.

AWS IoT

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS IoT	`AWS::IoT::Authorizer`	N/D	N/D
	`AWS::IoT::SecurityProfile`	N/D	N/D
	`AWS::IoT::RoleAlias`	N/D	N/D
	`AWS::IoT::Dimension`	N/D	N/D
	`AWS::IoT::Policy`	N/D	N/D
	`AWS::IoT::MitigationAction`	N/D	N/D
	`AWS::IoT::ScheduledAudit`	N/D	N/D
	`AWS::IoT::AccountAuditConfiguration`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::IoTSiteWise::Gateway`	N/D	N/D
	`AWS::IoT::CustomMetric`	N/D	N/D
	`AWS::IoT::JobTemplate`	N/D	N/D
	`AWS::IoT::ProvisioningTemplate`	N/D	N/D
	`AWS::IoT::CACertificate`	N/D	N/D
AWS IoT Wireless	`AWS::IoTWireless::ServiceProfile`	N/D	N/D
	`AWS::IoTWireless::MulticastGroup`	N/D	N/D
	`AWS::IoTWireless::FuotaTask`	N/D	N/D
AWS IoT Core	`AWS::IoT::FleetMetric`	N/D	N/D
AWS IoT Analytics	`AWS::IoTAnalytics::Datastore`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::IoTAnalytics::Dataset`	N/D	N/D
	`AWS::IoTAnalytics::Pipeline`	N/D	N/D
	`AWS::IoTAnalytics::Channel`	N/D	N/D
AWS IoT Events	`AWS::IoTEvents::Input`	N/D	N/D
	`AWS::IoTEvents::DetectorModel`	N/D	N/D
	`AWS::IoTEvents::AlarmModel`	N/D	N/D
AWS IoT TwinMaker	`AWS::IoTTwinMaker::Workspace`	N/D	N/D
	`AWS::IoTTwinMaker::Entity`	N/D	N/D
	`AWS::IoTTwinMaker::Scene`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::IoTTwinMaker::SyncJob`	N/D	N/D
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	N/D	N/D
	`AWS::IoTSiteWise::Project`	N/D	N/D
	`AWS::IoTSiteWise::Portal`	N/D	N/D
	`AWS::IoTSiteWise::AssetModel`	N/D	N/D
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	N/D	N/D

AWS Key Management Service

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Key Management Service	`AWS::KMS::Key`	N/D	N/D
	`AWS::KMS::Alias`	N/D	N/D

AWS Lambda

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Lambda	`AWS::Lambda::Function`	está associado a	IAM role (Perfil do IAM)
			Security group EC2
		está contido em	Sub-rede EC2
	`AWS::Lambda::Alias`	N/D	N/D
	`AWS::Lambda::CodeSigningConfig`	N/D	N/D

AWS Mainframe Modernization

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Mainframe Modernization	`AWS::M2::Environment`	N/D	N/D

AWS Network Firewall

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	é anexado a	Sub-rede EC2
		está associado a	NetworkFirewall FirewallPolicy

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::NetworkFirewall::FirewallPolicy`	está associado a	NetworkFirewall RuleGroup
	`AWS::NetworkFirewall::RuleGroup`	N/D	N/D
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	N/D	N/D

AWS Network Manager

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	N/D	N/D
	`AWS::NetworkManager::Site`	N/D	N/D
	`AWS::NetworkManager::Device`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::NetworkManager::Link`	N/D	N/D
	`AWS::NetworkManager::GlobalNetwork`	N/D	N/D
	`AWS::NetworkManager::CustomerGatewayAssociation`	N/D	N/D
	`AWS::NetworkManager::LinkAssociation`	N/D	N/D
	`AWS::NetworkManager::ConnectPeer`	N/D	N/D

AWS Panorama

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Panorama	`AWS::Panorama::Package`	N/D	N/D

AWS Private Certificate Authority

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`	N/D	N/D
	`AWS::ACMPCA::CertificateAuthorityActivation`	N/D	N/D

AWS Resilience Hub

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Resilience Hub	`AWS::ResilienceHub::ResiliencyPolicy`	N/D	N/D
	`AWS::ResilienceHub::App`	N/D	N/D

Explorador de recursos da AWS

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Explorador de recursos da AWS	`AWS::ResourceExplorer2::Index`	N/D	N/D

AWS RoboMaker

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	N/D	N/D
	`AWS::RoboMaker::RobotApplication`	N/D	N/D
	`AWS::RoboMaker::SimulationApplication`	N/D	N/D

AWS Signer

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Signer	`AWS::Signer::SigningProfile`	N/D	N/D

AWS Secrets Manager

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Secrets Manager	`AWS::SecretsManager::Secret`	está associado a	Função Lambda
		está associado a	Chave do KMS

AWS Service Catalog

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	está contido em	Portfólio
		está associado a	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationP`	está associado a	Portfólio
			CloudFormationProduto
			CloudFormationPilha

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`rovisionedProduct`		
	`AWS::ServiceCatalog::Portfolio`	contém	CloudFormationProduto

AWS Shield

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Shield	`AWS::Shield::Protection`	está associado a	CloudFront Distribuição da Amazon
	`AWS::ShieldRegional::Protection`	está associado a	EC2 EIP
		está associado a	ElasticLoadBalancing Balanceador
		está associado a	ElasticLoadBalanceamento V2 LoadBalancer

AWS Step Functions

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Step Functions	`AWS::StepFunctions::Activity`	N/D	N/D

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
	`AWS::Step Functions ::StateMachine`	N/D	N/D

AWS Systems Manager

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Systems Manager	`AWS::SSM: :ManagedI nstanceIn ventory` *	está associado a	EC2 instance (Instância do EC2)
	`AWS::SSM: :PatchCom pliance`	está associado a	Inventário de instância gerenciada
	`AWS::SSM: :Associat ionCompliance`	está associado a	Inventário de instância gerenciada
	`AWS::SSM: :FileData`	está associado a	Inventário de instância gerenciada
	`AWS::SSM: :Document`	N/D	N/D

*Para saber mais sobre o inventário de instância gerenciada, consulte Recording Software Configuration for Managed Instances.

AWS Transfer Family

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Transfer Family	`AWS::Transfer::Agreement`	N/D	N/D
	`AWS::Transfer::Connector`	N/D	N/D
	`AWS::Transfer::Workflow`	N/D	N/D
	`AWS::Transfer::Certificate`	N/D	N/D
	`AWS::Transfer::Profile`	N/D	N/D

AWS WAF

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS WAF	`AWS::WAF::RateBasedRule`	N/D	N/D
	`AWS::WAF::Rule`	N/D	N/D
	`AWS::WAF::WebACL`	está associado a	Regra do WAF
			Regra com base em taxa do WAF

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			Grupo de regras do WAF
	`AWS::WAF::RuleGroup`	está associado a	Regra do WAF
	`AWS::WAFRegional::RateBasedRule`	N/D	N/D
	`AWS::WAFRegional::Rule`	N/D	N/D
	`AWS::WAFRegional::WebACL`	está associado a	ElasticLoadBalancamento V2 LoadBalancer
			Regra do WAFRegional
			Regra com base em taxa do WAFRegional
			Grupo de regras do WAFRegional
	`AWS::WAFRegional::RuleGroup`	está associado a	Regra do WAFRegional
AWS WAF V2	`AWS::WAFv2::WebACL`	está associado a	ElasticLoadBalancamento V2 LoadBalancer
			ApiGateway Palco

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	está associado a	WAFv2 IPSet
			WAFv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	está associado a	WAFv2 RuleGroup
	`AWS::WAFv2::IPSet`	N/D	N/D
	`AWS::WAFv2::RegexPatternSet`	N/D	N/D

AWS X-Ray

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS X-Ray	`AWS::XRay::EncryptionConfig`	N/D	N/D

Elastic Load Balancing

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
Elastic Load Balancing	Application Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	está associado a	Security group EC2
		é anexado a	Sub-rede
		está contido em	Virtual private cloud (VPC)
	Receptor do Application Load Balancer `AWS::ElasticLoadBalancingV2::Listener`	N/D	N/D
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	está associado a	Security group EC2
		é anexado a	Sub-rede
		está contido em	Virtual private cloud (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	N/D	N/D

AWS Elemental MediaConnect

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	N/D	N/D
	`AWS::MediaConnect::FlowVpcInterface`	N/D	N/D
	`AWS::MediaConnect::FlowSource`	N/D	N/D

AWS Elemental MediaPackage

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	N/D	N/D
	`AWS::MediaPackage::PackagingConfiguration`	N/D	N/D

AWS Elemental MediaTailor

AWS Serviço	Valor de tipo de recurso	Relacionamento	Recurso relacionado
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	N/D	N/D

Cobertura de recursos por região e disponibilidade

Regiões da América do Norte e da América do Sul

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ACM::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthority	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ACMPCA::CertificateAuthorityAtivação	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::APS::RuleGroupsNamespace	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::AccessAnalyzer::Analyzer	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AmazonMQ::Broker	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Amplify::App	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Amplify::Branch	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ApiGateway::RestApi	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ApiGateway::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ApiGatewayV2::Api	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ApiGatewayV2::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppConfig::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppConfig::ConfigurationProfile	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppConfig::DeploymentStrategy	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::AppConfig::Environment	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppConfig::ExtensionAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppFlow::Flow	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppIntegrations::EventIntegration	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::AppMesh::GatewayRoute	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::AppMesh::Mesh	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppMesh::Route	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppMesh::VirtualGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppMesh::VirtualNode	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppMesh::VirtualRouter	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AppMesh::VirtualService	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::AppRunner::Service	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::AppRunner::VpcConnector	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::AppStream::Application	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::AppStream::DirectoryConfig	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::AppStream::Fleet	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::AppStream::Stack	Sim	Não	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::AppSync::GraphQLAPI	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Athena::DataCatalog	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Athena::PreparedStatement	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Athena::WorkGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::AuditManager::Assessment	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::AutoScaling::LaunchConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScalingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScheduledAction	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::WarmPool	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Backup::BackupPlan	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Backup::BackupSelection	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Backup::BackupVault	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Backup::RecoveryPoint	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Backup::ReportPlan	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Batch::ComputeEnvironment	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Batch::JobQueue	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Batch::SchedulingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Budgets::BudgetsAction	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::Cassandra::Keyspace	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Cloud9::EnvironmentEC2	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CloudFormation::Stack	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CloudFront::Distribution	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::CloudFront::StreamingDistribution	Nº	Nº	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::CloudTrail::Trail	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CloudWatch::Alarm	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CloudWatch::MetricStream	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CodeArtifact::Repository	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::CodeBuild::Project	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CodeBuild::ReportGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::CodeDeploy::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CodeDeploy::DeploymentConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CodeDeploy::DeploymentGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::CodeGuruProfiler::ProfilingGroup	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::CodeGuruReviewer::RepositoryAssociation	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::CodePipeline::Pipeline	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Cognito::UserPool	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Cognito::UserPoolCliente	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Cognito::UserPoolGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Config::ConfigurationRecorder	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Config::ConformancePackConformidade	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Config::ResourceCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Connect::Instance	Não	Nº	Sim	Sim	Não	Sim	Não
AWS::Connect::PhoneNumber	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Connect::QuickConnect	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::CustomerProfiles::Domain	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::CustomerProfiles::ObjectType	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::DMS::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::DMS::Endpoint	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DMS::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DMS::ReplicationInstance	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DMS::ReplicationSubnetGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DMS::ReplicationTask	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationEFS	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::DataSync::LocationF SxLustre	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationF SxWindows	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationHDFS	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationNFS	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationObjectArmazenamento	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::LocationS3	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::DataSync::LocationSMB	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DataSync::Task	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Detective::Graph	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::DeviceFarm::InstanceProfile	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::DeviceFarm::Project	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::DeviceFarm::TestGridProjeto	Nº	Nº	Nº	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::DynamoDB::Table	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Capacity Reservation	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::CarrierGateway	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::EC2::ClientVpnPonto final	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::CustomerGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::EC2Fleet	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::EIP	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EgressOnlyInternetGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::FlowLog	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::Host	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAM	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::IPAMPool	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::IPAMScope	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::Instance	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::InternetGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::NatGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::NetworkAcl	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::NetworkInsightsAccessScope	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::NetworkInsightsAccessScopeAnálise	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::NetworkInsightsAnálise	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::NetworkInsightsCaminho	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::NetworkInterface	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::PrefixList	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::RegisteredInstância HA	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::RouteTable	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SpotFleet	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::Subnet	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TrafficMirrorFiltrar	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TrafficMirrorSessão	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TrafficMirrorAlvo	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TransitGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayAnexo	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EC2::TransitGatewayConnect	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayRouteTable	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EC2::VPC	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPCEndpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :EC2: :VPC EndpointService	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS: :EC2: :VPC PeeringConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPNConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPNGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Volume	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::PublicRepository	Não	Nº	Sim	Não	Nº	Nº	Nº
AWS::ECR::PullThroughCacheRule	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ECR::RegistryPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ECR::Repository	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ECS::CapacityProvider	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ECS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::Service	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::TaskDefinition	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ECS::TaskSet	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EFS::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EFS::FileSystem	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EKS::Addon	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EKS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EKS::FargateProfile	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EKS::Identity ProviderConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EMR::Security Configuration	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ElasticBeanstalk::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ElasticBeanstalk::ApplicationVersion	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ElasticBeanstalk::Environment	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ElasticLoadBalancingV2::Listener	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Elasticsearch::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EventSchemas::Discoverer	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EventSchemas::Registry	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::EventSchemas::RegistryPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::EventSchemas::Schema	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Events::ApiDestination	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Events::Archive	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Events::Connection	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Events::Endpoint	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Events::EventBus	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Events::Rule	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Evidently::Launch	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::Evidently::Project	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::Evidently::Segment	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::FIS::ExperimentTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Forecast::Dataset	Sim	Não	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Forecast::DatasetGroup	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::FraudDetector::EntityType	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::FraudDetector::Label	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::FraudDetector::Outcome	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::FraudDetector::Variable	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::GlobalAccelerator::Accelerator	Nº	Nº	Nº	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::GlobalAccelerator::EndpointGroup	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::GlobalAccelerator::Listener	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Glue::Classifier	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Glue::Job	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Glue: :Transformação de ML	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Grafana::Workspace	Sim	Não	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::GreengrassV2::ComponentVersion	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::GroundStation::Config	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::GroundStation::DataflowEndpointGrupo	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::GroundStation::MissionProfile	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::GuardDuty::Detector	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::GuardDuty::Filter	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::GuardDever: :IPset	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::GuardDuty::ThreatIntelConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::HealthLake: :Armazenamento de dados FHIR	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::IAM::Group	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IAM::InstanceProfile	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::IAM::OIDCProvider	Nº	Nº	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IAM::Policy	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IAM::Role	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IAM::SAMLProvider	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::IAM::ServerCertificate	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::IAM::User	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IVS::Channel	Nº	Nº	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IVS::PlaybackKeyPar	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::IVS::RecordingConfiguration	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::ImageBuilder::ContainerRecipe	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ImageBuilder::ImagePipeline	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ImageBuilder::ImageRecipe	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ImageBuilder: :InfrastructureConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::InspectorV2::Filter	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::AccountAuditConfiguração	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::IoT::Authorizer	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoCertificado T: :CA	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::CustomMetric	Sim	Não	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IoT::Dimension	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::IoT::FleetMetric	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::JobTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::MitigationAction	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::IoT::Policy	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::ProvisioningTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IoT::RoleAlias	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::IoT::ScheduledAudit	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::IoT::SecurityProfile	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::IoTAnalytics::Channel	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::IoTAnalytics::Dataset	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::IoTAnalytics::Datastore	Sim	Não	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IoTAnalytics::Pipeline	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::IoTEvents::AlarmModel	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTEvents::DetectorModel	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTEvents::Input	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTSiteWise::AssetModel	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTSiteWise::Dashboard	Sim	Não	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IoTSiteWise::Gateway	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTSiteWise::Portal	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTSiteWise::Project	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::IoTTwinMaker::ComponentType	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::IoTTwinMaker::Entity	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::IoTTwinMaker::Scene	Nº	Nº	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::IoTTwinMaker::SyncJob	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::IoTTwinMaker::Workspace	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::IoTWireless::FuotaTask	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTWireless::MulticastGroup	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTWireless::ServiceProfile	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::KMS::Alias	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::KMS::Key	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::KafkaConnect::Connector	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Kendra::Index	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Kinesis::Stream	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Kinesis::StreamConsumer	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::KinesisAnalyticsV2::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::KinesisFirehose::DeliveryStream	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::KinesisVideo::SignalingChannel	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::KinesisVideo::Stream	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::Lambda::CodeSigningConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Lambda::Function	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Lex::Bot	Não	Nº	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Lex::BotAlias	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Lightsail::Bucket	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Lightsail::Certificate	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Lightsail::Disk	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Lightsail::StaticIp	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Logs::Destination	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::LookoutMetrics::Alert	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::LookoutVision::Project	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::M2::Environment	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MSK::BatchScramSegredo	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MSK::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MSK::ClusterPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::MSK::Configuration	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MSK::VpcConnection	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MediaConnect::FlowEntitlement	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MediaConnect::FlowSource	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MediaConnect::FlowVpcInterface	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::MediaPackage::PackagingConfiguration	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::MediaPackage::PackagingGroup	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::MediaTailor::PlaybackConfiguration	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::MemoryDB::SubnetGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::NetworkFirewall::Firewall	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::NetworkFirewall::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::NetworkManager::ConnectPeer	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::CustomerGateway Associação	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::Device	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::GlobalNetwork	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::Link	Nº	Nº	Nº	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::NetworkManager::LinkAssociation	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::Site	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::NetworkManager::TransitGatewayRegistro	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::OpenSearch::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Panorama::Package	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Personalize::Dataset	Sim	Não	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Personalize::DatasetGroup	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Personalize::Schema	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Personalize::Solution	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::App	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::ApplicationSettings	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::Campaign	Nº	Nº	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Pinpoint::EmailChannel	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::EmailTemplate	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::EventStream	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::InAppModelo	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::Pinpoint::Segment	Nº	Nº	Sim	Sim	Não	Sim	Não
AWS::QLDB::Ledger	Sim	Não	Sim	Sim	Não	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::QuickSight::DataSource	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::QuickSight::Template	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::QuickSight::Theme	Sim	Sim	Sim	Sim	Não	Sim	Não
AWS::RDS::DBCluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::DBInstance	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS: :RDS: :DB SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::DBSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SubnetGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::GlobalCluster	Sim	Não	Sim	Sim	Sim	Sim	Não
AWS::RDS::OptionGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::RUM::AppMonitor	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::Redshift::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterParameterGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Redshift::EndpointAccess	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Redshift::EndpointAuthorization	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Redshift::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ScheduledAction	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ResilienceHub::App	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ResilienceHub::ResiliencyPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ResourceExplorer2::Index	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::RoboMaker::RobotApplication	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::RoboMaker::RobotApplicationVersão	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::RoboMaker::SimulationApplication	Sim	Não	Sim	Sim	Não	Nº	Nº
AWS::Route53::HealthCheck	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::Route53::HostedZone	Nº	Nº	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Route53RecoveryControl::Cluster	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryControl::ControlPanel	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryControl::RoutingControl	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryControl::SafetyRule	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryReadiness::Cell	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryReadiness::ReadinessCheck	Nº	Nº	Nº	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Route53RecoveryReadiness::RecoveryGroup	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53RecoveryReadiness::ResourceSet	Nº	Nº	Nº	Sim	Não	Nº	Nº
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::FirewallRuleGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverEndpoint	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverRule	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::S3::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::S3::AccountPublicAccessBlock	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::S3::Bucket	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::MultiRegionAccessPoint	Não	Nº	Nº	Sim	Não	Nº	Nº
AWS::S3::StorageLens	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SES::ConfigurationSet	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SES::ContactList	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SES::ReceiptFilter	Nº	Nº	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::SES::ReceiptRuleConjunto	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::SES::Template	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SNS::Topic	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SQS::Queue	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SSM::AssociationCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SSM::Document	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::SSM::FileData	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SSM::ManagedInstanceInventário	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SSM::PatchCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::AppImageConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::CodeRepository	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::SageMaker::EndpointConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::FeatureGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::Image	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::Model	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::NotebookInstance	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::SageMaker::Workteam	Sim	Não	Sim	Sim	Não	Sim	Não
AWS::SecretsManager::Secret	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceCatalog::CloudFormationProduto	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceCatalog::Portfolio	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::HttpNamespace	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::ServiceDiscovery::Instance	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::PublicDnsNamespace	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::Service	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Shield::Protection	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::ShieldRegional::Protection	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Signer::SigningProfile	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::StepFunctions::Activity	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::StepFunctions::StateMachine	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Transfer::Agreement	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Transfer::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Transfer::Connector	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::Transfer::Profile	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::Transfer::Workflow	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAF::RateBasedRegra	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::WAF::Rule	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::WAF::RuleGroup	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::WAF::WebACL	Nº	Nº	Sim	Não	Nº	Nº	Nº
AWS::WAFRegional::RateBasedRegra	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::WAFRegional::Rule	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFRegional::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFRegional::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFv2::IPSet	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFv2::RegexPatternConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Não

Tipo de atributo	Oeste dos EUA (Norte da Califórnia)	Leste dos EUA (Norte da Virgínia)	Oeste dos EUA (Oregon)	Leste dos EUA (Ohio)	Oeste do Canadá (Calgary)	Canadá (Central)	América do Sul (São Paulo)
AWS::WAFv2::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WAFv2::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Não
AWS::WorkSpaces::ConnectionAlias	Nº	Sim	Sim	Sim	Não	Sim	Não
AWS::WorkSpaces::Workspace	Nº	Sim	Sim	Sim	Não	Sim	Não
AWS::XRay::EncryptionConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não

Regiões da Europa

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::ACM::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthority	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthorityAtivação	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::APS::RuleGroupsNamespace	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::AccessAnalyzer::Analyzer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AmazonMQ::Broker	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Amplify::App	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Amplify::Branch	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ApiGateway::RestApi	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGateway::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Api	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppConfig::ConfigurationProfile	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppConfig::DeploymentStrategy	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::AppConfig::Environment	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppConfig::ExtensionAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppFlow::Flow	Nº	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::AppIntegrations::EventIntegration	Nº	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::AppMesh::GatewayRoute	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppMesh::Mesh	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppMesh::Route	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::AppMesh::VirtualGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualNode	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualRouter	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualService	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AppRunner::Service	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::AppRunner::VpcConnector	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::AppStream::Application	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::AppStream::DirectoryConfig	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::AppStream::Fleet	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::AppStream::Stack	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::AppSync::GraphQLAPI	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Athena::DataCatalog	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Athena::PreparedStatement	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Athena::WorkGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::AuditManager::Assessment	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::AutoScaling::LaunchConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScalingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScheduledAction	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Auto Scaling::WarmPool	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Backup::BackupPlan	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Backup::BackupSelection	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Backup::BackupVault	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Backup::RecoveryPoint	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Backup::ReportPlan	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Batch::ComputeEnvironment	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Batch::JobQueue	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Batch::SchedulingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Cassandra::Keyspace	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Cloud9::EnvironmentEC2	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CloudFormation::Stack	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CloudTrail::Trail	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::CloudWatch::Alarm	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CloudWatch::MetricStream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CodeArtifact::Repository	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CodeBuild::Project	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CodeBuild::ReportGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CodeDeploy::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CodeDeploy::DeploymentConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::CodeDeploy::DeploymentGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::CodeGuruProfiler::ProfilingGroup	Sim	Não	Sim	Sim	Sim	Não	Nº	Nº
AWS::CodeGuruReviewer::RepositoryAssociation	Sim	Não	Sim	Sim	Sim	Não	Nº	Nº
AWS::CodePipeline::Pipeline	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Cognito::UserPool	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Cognito::UserPoolCliente	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Cognito::UserPoolGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Config::ConfigurationRecorder	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Config::ConformancePackConformidade	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Config::ResourceCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Connect::Instance	Não	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::Connect::PhoneNumber	Nº	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::Connect::QuickConnect	Nº	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::CustomerProfiles::Domain	Nº	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::CustomerProfiles::ObjectType	Nº	Nº	Nº	Sim	Sim	Não	Nº	Nº
AWS::DMS::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DMS::Endpoint	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::DMS::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DMS::ReplicationInstance	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DMS::ReplicationSubnetGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DMS::ReplicationTask	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DataSync::LocationEFS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::LocationF SxLustre	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DataSync::LocationF SxWindows	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DataSync::LocationHDFS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::DataSync::LocationNFS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::LocationObjectArmazenamento	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::LocationS3	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::LocationSMB	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::Task	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Detective::Graph	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::DynamoDB::Table	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::CapacityReservation	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EC2::CarrierGateway	Nº	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EC2::ClientVpnPonto final	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::CustomerGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EC2Fleet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EIP	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EgressOnlyInternetGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
AWS::EC2::FlowLog	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EC2::Host	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAM	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAMPool	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAMScope	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Instance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::InternetGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::NatGateway	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EC2::NetworkAcl	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::NetworkInsightsAccessScope	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::NetworkInsightsAccessScopeAnálise	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::NetworkInsightsAnálise	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::NetworkInsightsCaminho	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::NetworkInterface	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::PrefixList	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::RegisteredInstância HA	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EC2::RouteTable	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SpotFleet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Subnet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TrafficMirrorFiltrar	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EC2::TrafficMirrorSessão	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EC2::TrafficMirrorAlvo	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EC2::TransitGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TransitGatewayAnexo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TransitGatewayConnect	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TransitGatewayRouteTable	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
AWS::EC2::VPC	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPCEndpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :EC2: :VPC EndpointService	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS: :EC2: :VPC PeeringConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2: :VPNConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPNGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Volume	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::PullThroughCacheRule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::RegistryPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::Repository	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS: :CapacityProvider	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::ECS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::Service	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::TaskDefinition	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::TaskSet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EFS::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EFS::FileSystem	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::Addon	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::EKS::FargateProfile	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::IdentityProviderConfig	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EMR::SecurityConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ElasticBeanstalk::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ElasticBeanstalk::ApplicationVersion	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ElasticBeanstalk::Environment	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ElasticLoadBalancingV2::Listener	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Elasticsearch::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EventSchemas::Discoverer	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EventSchemas::Registry	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EventSchemas::RegistryPolicy	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::EventSchemas::Schema	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Events::ApiDestination	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Events::Archive	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Events::Connection	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Events::Endpoint	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Events::EventBus	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Events::Rule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Evidently::Launch	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::Evidently::Project	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::Evidently::Segment	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::FIS::ExperimentTemplate	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Forecast::Dataset	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Forecast::DatasetGroup	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::FraudDetector::EntityType	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::FraudDetector::Label	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::FraudDetector::Outcome	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::FraudDetector::Variable	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::Glue::Classifier	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Glue::Job	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Glue: :Transformação de ML	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Grafana::Workspace	Não	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::GreengrassV2: :ComponentVersion	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::GroundStation::Config	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::GroundStation::DataflowEndpointGrupo	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::GroundStation::MissionProfile	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::GuardDuty::Detector	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::GuardDuty::Filter	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::GuardDever: :IPset	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::GuardDuty::ThreatIntelConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IAM::Group	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IAM::Policy	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IAM::Role	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IAM::User	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IVS::Channel	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IVS::PlaybackKeyPar	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::IVS::RecordingConfiguration	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::ImageBuilder::ContainerRecipe	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ImageBuilder::ImagePipeline	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ImageBuilder::ImageRecipe	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ImageBuilder::InfrastructureConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::InspectorV2::Filter	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::IoT::AccountAuditConfiguração	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::IoT::Authorizer	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoCertificado T: :CA	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::CustomMetric	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::Dimension	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::FleetMetric	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::JobTemplate	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::MitigationAction	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::Policy	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::IoT::ProvisioningTemplate	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::RoleAlias	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::ScheduledAudit	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoT::SecurityProfile	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTAnalytics::Channel	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTAnalytics::Dataset	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTAnalytics::Datastore	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTAnalytics::Pipeline	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::IoTEvents::AlarmModel	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTEvents::DetectorModel	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTEvents::Input	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::IoTSiteWise::AssetModel	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTSiteWise::Dashboard	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTSiteWise::Gateway	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTSiteWise::Portal	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTSiteWise::Project	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::IoTTwinMaker::ComponentType	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTTwinMaker::Entity	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTTwinMaker::Scene	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTTwinMaker::SyncJob	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTTwinMaker::Workspace	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTWireless::FuotaTask	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTWireless::MulticastGroup	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::IoTWireless::ServiceProfile	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::KMS::Alias	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::KMS::Key	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::KafkaConnect::Connector	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Kendra::Index	Nº	Nº	Sim	Não	Sim	Não	Nº	Nº
AWS::Kinesis::Stream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Kinesis::StreamConsumer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::KinesisAnalyticsV2::Application	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::KinesisFirehose::DeliveryStream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::KinesisVideo::SignalingChannel	Não	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::KinesisVideo::Stream	Nº	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Lambda::CodeSigningConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Lambda::Function	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Lex::Bot	Não	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Lex::BotAlias	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Lightsail::Bucket	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Lightsail::Certificate	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Lightsail::Disk	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Lightsail::StaticIp	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Logs::Destination	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::LookoutMetrics::Alert	Sim	Não	Sim	Sim	Não	Nº	Nº	Nº
AWS::LookoutVision::Project	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::M2::Environment	Nº	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::MSK::BatchScramSegredo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::MSK::ClusterPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::Configuration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::VpcConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MediaConnect::FlowEntitlement	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::MediaConnect::FlowSource	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::MediaConnect::FlowVpcInterface	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::MediaPackage::PackagingConfiguration	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::MediaPackage::PackagingGroup	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::MediaTailor::PlaybackConfiguration	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::MemoryDB::SubnetGroup	Sim	Não	Sim	Sim	Sim	Não	Nº	Nº
AWS::NetworkFirewall::Firewall	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::OpenSearch::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Panorama::Package	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Personalize::Dataset	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Personalize::DatasetGroup	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Personalize::Schema	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Personalize::Solution	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Pinpoint::App	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::ApplicationSettings	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::Campaign	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::EmailChannel	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Pinpoint::EmailTemplate	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::EventStream	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::InAppModelo	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::Pinpoint::Segment	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::QLDB::Ledger	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::QuickSight::DataSource	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::QuickSight::Template	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::QuickSight::Theme	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::RDS::DBCluster	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::DBInstance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::DBSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SubnetGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS: :EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS::GlobalCluster	Não	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::RDS::OptionGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RUM::AppMonitor	Sim	Não	Sim	Sim	Sim	Não	Nº	Nº
AWS::Redshift::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterParameterGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::EndpointAccess	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Redshift::EndpointAuthorization	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::Redshift::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ScheduledAction	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ResilienceHub::App	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ResilienceHub::ResiliencyPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ResourceExplorer2::Index	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::RoboMaker::RobotApplication	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::RoboMaker::RobotApplicationVersão	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::RoboMaker::SimulationApplication	Nº	Nº	Sim	Sim	Não	Nº	Nº	Nº
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Route53Resolver::FirewallRuleGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Route53Resolver::ResolverEndpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Route53Resolver::ResolverRule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::AccountPublicAccessBlock	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::S3::Bucket	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::StorageLens	Sim	Sim	Sim	Sim	Sim	Não	Nº	Nº
AWS::SES::ConfigurationSet	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SES::ContactList	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SES::ReceiptFilter	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::SES::ReceiptRuleConjunto	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::SES::Template	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SNS::Topic	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SQS::Queue	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SSM::AssociationCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SSM::Document	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SSM::FileData	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SSM::ManagedInstanceInventário	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::SSM::PatchCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SageMaker::AppImageConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::CodeRepository	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::EndpointConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::FeatureGroup	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::Image	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::Model	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::SageMaker::NotebookInstance	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::SageMaker::Workteam	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::SecretsManager::Secret	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::CloudFormationProduto	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::Portfolio	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceDiscovery::HttpNamespace	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::ServiceDiscovery::Instance	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ServiceDiscovery::PublicDnsNamespace	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ServiceDiscovery::Service	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::ShieldRegional::Protection	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Signer::SigningProfile	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::StepFunctions::Activity	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::StepFunctions::StateMachine	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Transfer::Agreement	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::Transfer::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Transfer::Connector	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::Transfer::Profile	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Transfer::Workflow	Sim	Sim	Sim	Sim	Sim	Sim	Não	Nº
AWS::WAFRegional::RateBasedRegra	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::Rule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Europa (Irlanda)	Europa (Frankfurt)	Europa (Londres)	Europa (Paris)	Europa (Estocolmo)	Europa (Milão)	Europa (Espanha)	Europa (Zurique)
AWS::WAFv2::IPSet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::RegexPatternConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WorkSpaces::ConnectionAlias	Não	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::WorkSpaces::Workspace	Nº	Nº	Sim	Sim	Sim	Não	Nº	Nº
AWS::XRay::EncryptionConfig	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Regiões da Ásia-Pacífico

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::ACM::Certificate	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthority	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthorityAtivação	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::APS::RuleGroupsNamespace	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AccessAnalyzer::Analyzer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AmazonMQ::Broker	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Amplify::App	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Amplify::Branch	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::ApiGateway::RestApi	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGateway::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Api	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Stage	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::Application	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::ConfigurationProfile	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::DeploymentStrategy	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::Environment	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::AppConfig::ExtensionAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AppFlow::Flow	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AppIntegrations::EventIntegration	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AppMesh::GatewayRoute	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppMesh::Mesh	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppMesh::Route	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppMesh::VirtualGateway	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::AppMesh::VirtualNode	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppMesh::VirtualRouter	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppMesh::VirtualService	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AppRunner::Service	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::AppRunner::VpcConnector	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Não	Nº
AWS::AppStream::Application	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AppStream::DirectoryConfig	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AppStream::Fleet	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::AppStream::Stack	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::AppSync::GraphQLAPI	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Athena::DataCatalog	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Athena::PreparedStatement	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Athena::WorkGroup	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::AuditManager::Assessment	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::LaunchConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::AutoScaling::ScalingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScheduledAction	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::AutoScaling::WarmPool	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Backup::BackupPlan	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Backup::BackupSelection	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Backup::BackupVault	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Backup::RecoveryPoint	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Backup::ReportPlan	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Batch::ComputeEnvironment	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Batch::JobQueue	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Batch::SchedulingPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Cassandra::Keyspace	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Cloud9::EnvironmentEC2	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::CloudFormation::Stack	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::CloudTrail::Trail	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CloudWatch::Alarm	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::CloudWatch::MetricStream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CodeArtifact::Repository	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::CodeBuild::Project	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::CodeBuild::ReportGroup	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::CodeDeploy::Application	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::CodeDeploy::DeploymentConfig	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::CodeDeploy::DeploymentGroup	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::CodeGuruProfiler::ProfilingGroup	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::CodeGuruReviewer::RepositoryAssociation	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::CodePipeline::Pipeline	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Cognito::UserPool	Sim	Não	Nº	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::Cognito::UserPoolCliente	Sim	Não	Nº	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::Cognito::UserPoolGrupo	Sim	Não	Nº	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::Config::ConfigurationRecorder	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Config::ConformancePackConformidade	Sim	Não	Sim	Não	Sim	Não	Sim	Sim	Sim	Sim
AWS::Config::ResourceCompliance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Connect::Instance	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Connect::PhoneNumber	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Connect::QuickConnect	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::CustomerProfiles::Domain	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::CustomerProfiles::ObjectType	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::DMS::Certificate	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DMS::Endpoint	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DMS::EventSubscription	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::DMS::ReplicationInstance	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DMS::ReplicationSubnetGrupo	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DMS::ReplicationTask	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationEFS	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationF SxLustre	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationF SxWindows	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationHDFS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::DataSync::LocationNFS	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::DataSync::LocationObjectArmazenamento	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationS3	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::LocationSMB	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::DataSync::Task	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Detective::Graph	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::DynamoDB::Table	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::CapacityReservation	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::CarrierGateway	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Não	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::ClientVpnPonto final	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::CustomerGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::EC2Fleet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EIP	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::EgressOnlyInternetGateway	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::FlowLog	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::Host	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::IPAM	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAMPool	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::IPAMScope	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Instance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::InternetGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::NatGateway	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::NetworkAcl	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::NetworkInsightsAccessScope	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::NetworkInsightsAccessScopeAnálise	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::NetworkInsightsAnálise	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::NetworkInsightsCaminho	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::NetworkInterface	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::PrefixList	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::RegisteredInstância HA	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::RouteTable	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SpotFleet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Subnet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TrafficMirrorFiltrar	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::TrafficMirrorSessão	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::TrafficMirrorAlvo	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EC2::TransitGateway	Sim	Sim	Sim	Sim	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::TransitGatewayAnexo	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::TransitGatewayConnect	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::TransitGatewayRouteTable	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::EC2::VPC	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPCEndpoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPCEndpointService	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPCPeeringConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EC2::VPNConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::VPNGateway	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EC2::Volume	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::PullThroughCacheRule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::RegistryPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECR::Repository	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::CapacityProvider	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::ECS::Service	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::TaskDefinition	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ECS::TaskSet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EFS::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EFS::FileSystem	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::Addon	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EKS::FargateProfile	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::EKS::IdentityProviderConfig	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EMR::SecurityConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ElasticBeanstalk::Application	Sim	Sim	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ElasticBeanstalk::ApplicationVersion	Sim	Sim	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ElasticBeanstalk::Environment	Sim	Sim	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ElasticLoadBalancingV2::Listener	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Elasticsearch::Domain	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::EventSchemas::Discoverer	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EventSchemas::Registry	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EventSchemas::RegistryPolicy	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::EventSchemas::Schema	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Events::ApiDestination	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Events::Archive	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Events::Connection	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Events::Endpoint	Sim	Não	Nº	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::Events::EventBus	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Events::Rule	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Evidently::Launch	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::Evidently::Project	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::Evidently::Segment	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::FIS::ExperimentTemplate	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Forecast::Dataset	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Forecast::DatasetGroup	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::FraudDetector::EntityType	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::FraudDetector::Label	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::FraudDetector::Outcome	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::FraudDetector::Variable	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::Glue::Classifier	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Glue::Job	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Glue: :Transformação de ML	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Grafana::Workspace	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::GreengrassV2::ComponentVersion	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::GroundStation::Config	Não	Nº	Nº	Nº	Sim	Não	Nº	Nº	Sim	Sim
AWS::GroundStation::DataflowEndpointGrupo	Nº	Nº	Nº	Nº	Sim	Não	Nº	Nº	Sim	Sim
AWS::GroundStation::MissionProfile	Não	Nº	Nº	Nº	Sim	Não	Nº	Nº	Sim	Sim
AWS::GuardDuty::Detector	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::GuardDuty::Filter	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::GuardDever: :IPset	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::GuardDuty::ThreatIntelConjunto	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::HealthLake: :Armazenamento de dados FHIR	Sim	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Nº
AWS::IAM::Group	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::IAM::Policy	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::IAM::Role	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::IAM::User	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::IVS::Channel	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Não	Nº
AWS::IVS: :PlaybackKeyPar	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Não	Nº

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::IVS::RecordingConfiguration	Sim	Não	Nº	Nº	Sim	Não	Nº	Nº	Nº	Nº
AWS::ImageBuilder::ContainerRecipe	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::ImageBuilder::ImagePipeline	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ImageBuilder::ImageRecipe	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::ImageBuilder::InfrastructureConfiguration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::InspectorV2::Filter	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::AccountAuditConfiguração	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::IoT::Authorizer	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoCertificado T: :CA	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::CustomMetric	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::Dimension	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::FleetMetric	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::JobTemplate	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::MitigationAction	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::Policy	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::IoT::ProvisioningTemplate	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::RoleAlias	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::ScheduledAudit	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoT::SecurityProfile	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTAnalytics::Channel	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim
AWS::IoTAnalytics::Dataset	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim
AWS::IoTAnalytics::Datastore	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim
AWS::IoTAnalytics::Pipeline	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::IoTEvents::AlarmModel	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTEvents::DetectorModel	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTEvents::Input	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTSiteWise::AssetModel	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTSiteWise::Dashboard	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTSiteWise::Gateway	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTSiteWise::Portal	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::IoTSiteWise::Project	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::IoTTwinMaker::ComponentType	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::IoTTwinMaker::Entity	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::IoTTwinMaker::Scene	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::IoTTwinMaker::SyncJob	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::IoTTwinMaker::Workspace	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim
AWS::IoTWireless::FuotaTask	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim
AWS::IoTWireless::MulticastGroup	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim
AWS::IoTWireless::ServiceProfile	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Não	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::KMS::Alias	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::KMS::Key	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::KafkaConnect::Connector	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Kendra::Index	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::Kinesis::Stream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Kinesis::StreamConsumer	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::KinesisAnalyticsV2::Application	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::KinesisFirehose::DeliveryStream	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::KinesisVideo::SignalingChannel	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::KinesisVideo::Stream	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lambda::CodeSigningConfig	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lambda::Function	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Lex::Bot	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lex::BotAlias	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lightsail::Bucket	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lightsail::Certificate	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Lightsail::Disk	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Lightsail::StaticIp	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Logs::Destination	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::LookoutMetrics::Alert	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::LookoutVision::Project	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Não	Nº
AWS::M2::Environment	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::MSK::BatchScramSegredo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::MSK::ClusterPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::Configuration	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MSK::VpcConnection	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::MediaConnect::FlowEntitlement	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::MediaConnect::FlowSource	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::MediaConnect::FlowVpcInterface	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::MediaPackage::PackagingConfiguration	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::MediaPackage::PackagingGroup	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::MediaTailor::PlaybackConfiguration	Sim	Não	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::MemoryDB::SubnetGroup	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::NetworkFirewall::Firewall	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::OpenSearch::Domain	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Panorama::Package	Não	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Personalize::Dataset	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Personalize::DatasetGroup	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Personalize::Schema	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Personalize::Solution	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::App	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::ApplicationSettings	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::Campaign	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::EmailChannel	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Pinpoint::EmailTemplate	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::EventStream	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::InAppModelo	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Pinpoint::Segment	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::QLDB::Ledger	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::QuickSight::DataSource	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::QuickSight::Template	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::QuickSight::Theme	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::RDS::DBCluster	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS: :DBInstance	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SecurityGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS: :DBSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SubnetGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS: :EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RDS: :GlobalCluster	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::RDS::OptionGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::RUM::AppMonitor	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Sim
AWS::Redshift::Cluster	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterParameterGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSnapshot	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::EndpointAccess	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Redshift::EndpointAuthorization	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::Redshift::EventSubscription	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Redshift::ScheduledAction	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ResilienceHub::App	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ResilienceHub::ResiliencyPolicy	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ResourceExplorer2::Index	Sim	Não	Nº	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::RoboMaker::RobotApplication	Não	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Não
AWS::RoboMaker::RobotApplicationVersão	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Não

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::RoboMaker::SimulationApplication	Nº	Nº	Nº	Nº	Nº	Nº	Nº	Sim	Sim	Não
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Route53Resolver::FirewallRuleGrupo	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Route53Resolver::ResolverEndpoint	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Route53Resolver::ResolverRule	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::AccessPoint	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::AccountPublicAccessBlock	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::S3::Bucket	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::S3::StorageLens	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::SES::ConfigurationSet	Sim	Sim	Não	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::SES::ContactList	Sim	Sim	Não	Nº	Sim	Sim	Não	Sim	Sim	Sim
AWS::SES::Template	Sim	Sim	Não	Nº	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::SNS::Topic	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SQS::Queue	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SSM::AssociationCompliance	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
AWS::SSM::Document	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SSM::FileData	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
AWS::SSM::ManagedInstanceInventário	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::SSM::PatchCompliance	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim
AWS::SageMaker::AppImageConfig	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::SageMaker::CodeRepository	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::Domain	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::EndpointConfig	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::FeatureGroup	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::Image	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::SageMaker::Model	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::NotebookInstance	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sim	Não	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::SageMaker::Workteam	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::SecretsManager::Secret	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::CloudFormationProduto	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::Portfolio	Sim	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::ServiceDiscovery::HttpNamespace	Sim	Não	Sim	Não	Sim	Não	Sim	Sim	Sim	Sim
AWS::ServiceDiscovery::Instance	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ServiceDiscovery::PublicDnsNamespace	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::ServiceDiscovery::Service	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::ShieldRegional::Protection	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Signer::SigningProfile	Sim	Não	Sim	Não	Sim	Não	Nº	Sim	Sim	Sim
AWS::StepFunctions::Activity	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::StepFunctions::StateMachine	Sim	Sim	Sim	Sim	Sim	Sim	Não	Sim	Sim	Sim
AWS::Transfer::Agreement	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Transfer::Certificate	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::Transfer::Connector	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::Transfer::Profile	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::Transfer::Workflow	Sim	Sim	Sim	Não	Sim	Sim	Não	Sim	Sim	Sim
AWS::WAFRegional::RateBasedRegra	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::Rule	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFRegional::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::IPSet	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Tipo de atributo	Ásia-Pacífico (Singapura)	Ásia-Pacífico (Tóquio)	Ásia-Pacífico (Sydney)	Ásia-Pacífico (Seul)	Ásia Pacífico (Mumbai)	Asia Pacific (Osaka)	Ásia-Pacífico (Hong Kong)	Ásia-Pacífico (Jacarta)	Ásia-Pacífico (Hyderabad)	Ásia-Pacífico (Melbourne)
AWS::WAFv2::RegexPatternConjunto	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::RuleGroup	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WAFv2::WebACL	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
AWS::WorkSpaces::ConnectionAlias	Não	Nº	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::WorkSpaces::Workspace	Sim	Não	Nº	Nº	Sim	Não	Nº	Sim	Sim	Sim
AWS::XRay::EncryptionConfig	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Regiões da China

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::ACM::Certificate	Sim	Sim
AWS::AmazonMQ::Broker	Sim	Sim
AWS::ApiGateway::RestApi	Sim	Sim
AWS::ApiGateway::Stage	Sim	Sim
AWS::ApiGatewayV2::Api	Sim	Sim
AWS::ApiGatewayV2::Stage	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::AppConfig::Application	Sim	Sim
AWS::AppConfig::ConfigurationProfile	Sim	Sim
AWS::AppConfig::DeploymentStrategy	Sim	Sim
AWS::AppConfig::Environment	Sim	Sim
AWS::AppConfig::ExtensionAssociation	Sim	Sim
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim
AWS::AppSync::GraphQLAPI	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Athena::DataCatalog	Sim	Sim
AWS::Athena::PreparedStatement	Sim	Sim
AWS::Athena::WorkGroup	Sim	Sim
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim
AWS::AutoScaling::LaunchConfiguration	Sim	Sim
AWS::AutoScaling::ScalingPolicy	Sim	Sim
AWS::AutoScaling::ScheduledAction	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::AutoScaling::WarmPool	Sim	Sim
AWS::Backup::BackupPlan	Sim	Sim
AWS::Backup::BackupSelection	Sim	Sim
AWS::Backup::BackupVault	Sim	Sim
AWS::Backup::RecoveryPoint	Sim	Sim
AWS::Batch::ComputeEnvironment	Sim	Sim
AWS::Batch::JobQueue	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Batch::SchedulingPolicy	Sim	Sim
AWS::Cassandra::Keyspace	Sim	Sim
AWS::CloudFormation::Stack	Sim	Sim
AWS::CloudTrail::Trail	Sim	Sim
AWS::CloudWatch::Alarm	Sim	Sim
AWS::CloudWatch::MetricStream	Sim	Sim
AWS::CodeBuild::Project	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::CodeBuild::ReportGroup	Sim	Sim
AWS::Config::ConfigurationRecorder	Sim	Sim
AWS::Config::ResourceCompliance	Sim	Sim
AWS::DMS::Certificate	Sim	Sim
AWS::DMS::Endpoint	Sim	Sim
AWS::DMS::EventSubscription	Sim	Sim
AWS::DMS::ReplicationInstance	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::DMS::ReplicationSubnetGrupo	Sim	Sim
AWS::DMS::ReplicationTask	Sim	Sim
AWS::DataSync::LocationEFS	Sim	Sim
AWS::DataSync::LocationHDFS	Sim	Sim
AWS::DataSync::LocationNFS	Sim	Sim
AWS::DataSync::LocationObjectArmazenamento	Sim	Sim
AWS::DataSync::LocationS3	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::DataSync::LocationSMB	Sim	Sim
AWS::DataSync::Task	Sim	Sim
AWS::DynamoDB::Table	Sim	Sim
AWS::EC2::CapacityReservation	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim
AWS::EC2::EC2Fleet	Sim	Sim
AWS::EC2::EIP	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::EC2::FlowLog	Sim	Sim
AWS::EC2::Host	Sim	Sim
AWS::EC2::Instance	Sim	Sim
AWS::EC2::InternetGateway	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim
AWS::EC2::NatGateway	Sim	Sim
AWS::EC2::NetworkAcl	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::EC2::NetworkInterface	Sim	Sim
AWS::EC2::PrefixList	Sim	Sim
AWS::EC2::RouteTable	Sim	Sim
AWS::EC2::SecurityGroup	Sim	Sim
AWS::EC2::SpotFleet	Sim	Sim
AWS::EC2::Subnet	Sim	Sim
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::EC2::TrafficMirrorFiltrar	Sim	Sim
AWS::EC2::TrafficMirrorSessão	Sim	Sim
AWS::EC2::TrafficMirrorAlvo	Sim	Sim
AWS::EC2::TransitGateway	Sim	Sim
AWS::EC2::TransitGatewayAnexo	Sim	Sim
AWS::EC2::TransitGatewayConnect	Sim	Sim
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::EC2::TransitGatewayRouteTable	Sim	Sim
AWS::EC2::VPC	Sim	Sim
AWS::EC2::VPCEndpoint	Sim	Sim
AWS: :EC2: :VPC EndpointService	Sim	Sim
AWS: :EC2: :VPC PeeringConnection	Sim	Sim
AWS::EC2::VPNGateway	Sim	Não
AWS::EC2::Volume	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::ECR::Repository	Sim	Sim
AWS::ECS::CapacityProvider	Sim	Sim
AWS::ECS::Cluster	Sim	Sim
AWS::ECS::Service	Sim	Sim
AWS::ECS::TaskDefinition	Sim	Sim
AWS::ECS::TaskSet	Sim	Sim
AWS::EFS::AccessPoint	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::EFS::FileSystem	Sim	Sim
AWS::EKS::Addon	Sim	Sim
AWS::EKS::Cluster	Sim	Sim
AWS::EKS::FargateProfile	Sim	Sim
AWS::EKS::IdentityProviderConfig	Sim	Sim
AWS::EMR::SecurityConfiguration	Sim	Sim
AWS::ElasticBeanstalk::Application	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::ElasticBeanstalk::ApplicationVersion	Sim	Sim
AWS::ElasticBeanstalk::Environment	Sim	Sim
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim
AWS::ElasticLoadBalancingV2::Listener	Sim	Sim
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim
AWS::Elasticsearch::Domain	Sim	Sim
AWS::Events::Archive	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Events::EventBus	Sim	Sim
AWS::Events::Rule	Sim	Sim
AWS::Glue::Classifier	Sim	Sim
AWS::Glue::Job	Sim	Sim
AWS::Glue: :Transformação de ML	Sim	Não
AWS::GreengrassV2::ComponentVersion	Sim	Não
AWS::GuardDuty::Filter	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::GuardDuty::ThreatIntelConjunto	Sim	Sim
AWS::IAM::Group	Sim	Sim
AWS::IAM::InstanceProfile	Sim	Não
AWS::IAM::OIDCProvider	Sim	Não
AWS::IAM::Policy	Sim	Sim
AWS::IAM::Role	Sim	Sim
AWS::IAM::SAMLProvider	Sim	Não

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::IAM::ServerCertificate	Sim	Não
AWS::IAM::User	Sim	Sim
AWS::ImageBuilder::ContainerRecipe	Sim	Sim
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim
AWS::ImageBuilder::ImagePipeline	Sim	Sim
AWS::ImageBuilder::ImageRecipe	Sim	Sim
AWS::ImageBuilder::InfrastructureConfiguration	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::IoT::AccountAuditConfiguração	Sim	Sim
AWS::IoT::Authorizer	Sim	Sim
AWS::IoCertificado T: :CA	Sim	Sim
AWS::IoT::CustomMetric	Sim	Sim
AWS::IoT::Dimension	Sim	Sim
AWS::IoT::FleetMetric	Sim	Sim
AWS::IoT::JobTemplate	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::IoT::MitigationAction	Sim	Sim
AWS::IoT::Policy	Sim	Sim
AWS::IoT::ProvisioningTemplate	Sim	Sim
AWS::IoT::RoleAlias	Sim	Sim
AWS::IoT::ScheduledAudit	Sim	Sim
AWS::IoT::SecurityProfile	Sim	Sim
AWS::IoTAnalytics::Channel	Sim	Não

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::IoTAnalytics::Dataset	Sim	Não
AWS::IoTAnalytics::Datastore	Sim	Não
AWS::IoTAnalytics::Pipeline	Sim	Não
AWS::IoTEvents::AlarmModel	Sim	Não
AWS::IoTEvents::DetectorModel	Sim	Não
AWS::IoTEvents::Input	Sim	Não
AWS::IoTSiteWise::AssetModel	Sim	Não

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::IoTSiteWise::Dashboard	Sim	Não
AWS::IoTSiteWise::Gateway	Sim	Não
AWS::IoTSiteWise::Portal	Sim	Não
AWS::IoTSiteWise::Project	Sim	Não
AWS::KMS::Alias	Sim	Sim
AWS::KMS::Key	Sim	Sim
AWS::Kinesis::Stream	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Kinesis::StreamConsumer	Sim	Sim
AWS::KinesisAnalyticsV2::Application	Sim	Sim
AWS::KinesisFirehose::DeliveryStream	Sim	Sim
AWS::Lambda::Function	Sim	Não
AWS::Logs::Destination	Sim	Sim
AWS::MSK::BatchScramSegredo	Sim	Sim
AWS::MSK::Cluster	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::MSK::ClusterPolicy	Sim	Sim
AWS::MSK::Configuration	Sim	Sim
AWS::MSK::VpcConnection	Sim	Sim
AWS::NetworkFirewall::Firewall	Sim	Sim
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim
AWS::NetworkFirewall::RuleGroup	Sim	Sim
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::OpenSearch::Domain	Sim	Sim
AWS::Personalize::Dataset	Sim	Não
AWS::Personalize::DatasetGroup	Sim	Não
AWS::Personalize::Schema	Sim	Não
AWS::Personalize::Solution	Sim	Não
AWS::RDS::DBCluster	Nº	Sim
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::RDS::DBInstance	Sim	Sim
AWS: :RDS: :DB SecurityGroup	Sim	Sim
AWS::RDS::DBSnapshot	Sim	Sim
AWS: :RDS: :DB SubnetGroup	Sim	Sim
AWS::RDS::EventSubscription	Sim	Sim
AWS::RDS::OptionGroup	Sim	Sim
AWS::Redshift::Cluster	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Redshift::ClusterParameterGrupo	Sim	Sim
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim
AWS::Redshift::ClusterSnapshot	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim
AWS::Redshift::EventSubscription	Sim	Sim
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::Route53Resolver::ResolverEndpoint	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Sim
AWS::Route53Resolver::ResolverRule	Sim	Sim
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Sim
AWS::S3::AccessPoint	Sim	Sim
AWS::S3::AccountPublicAccessBlock	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::S3::Bucket	Sim	Sim
AWS::SES::ConfigurationSet	Não	Sim
AWS::SES::ContactList	Não	Sim
AWS::SES::Template	Não	Sim
AWS::SNS::Topic	Sim	Sim
AWS::SQS::Queue	Sim	Sim
AWS::SSM::AssociationCompliance	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::SSM::Document	Sim	Sim
AWS::SSM::FileData	Sim	Sim
AWS::SSM::ManagedInstanceInventário	Sim	Sim
AWS::SSM::PatchCompliance	Sim	Sim
AWS::SageMaker::AppImageConfig	Sim	Sim
AWS::SageMaker::CodeRepository	Sim	Sim
AWS::SageMaker::Domain	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::SageMaker::EndpointConfig	Sim	Sim
AWS::SageMaker::FeatureGroup	Sim	Sim
AWS::SageMaker::Image	Sim	Sim
AWS::SageMaker::Model	Sim	Sim
AWS::SageMaker::NotebookInstance	Sim	Sim
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sim	Sim
AWS::SecretsManager::Secret	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::ServiceCatalog::CloudFormationProduto	Sim	Sim
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Sim
AWS::ServiceCatalog::Portfolio	Sim	Sim
AWS::ServiceDiscovery::HttpNamespace	Sim	Sim
AWS::ServiceDiscovery::Instance	Sim	Sim
AWS::ServiceDiscovery::PublicDnsNamespace	Sim	Sim
AWS::ServiceDiscovery::Service	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::StepFunctions::Activity	Sim	Não
AWS::StepFunctions::StateMachine	Sim	Sim
AWS::Transfer::Agreement	Sim	Sim
AWS::Transfer::Certificate	Sim	Sim
AWS::Transfer::Connector	Sim	Sim
AWS::Transfer::Profile	Sim	Sim
AWS::Transfer::Workflow	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::WAFRegional::RateBasedRegra	Sim	Sim
AWS::WAFRegional::Rule	Sim	Sim
AWS::WAFRegional::RuleGroup	Sim	Sim
AWS::WAFRegional::WebACL	Sim	Sim
AWS::WAFv2::IPSet	Sim	Sim
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim
AWS::WAFv2::RegexPatternConjunto	Sim	Sim

Tipo de atributo	China (Pequim)	China (Ningxia)
AWS::WAFv2::RuleGroup	Sim	Sim
AWS::WAFv2::WebACL	Sim	Sim
AWS::WorkSpaces::Workspace	Não	Sim

Regiões da África e do Oriente Médio

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ACM::Certificate	Sim	Sim	Sim	Sim
AWS::ACMPCA::CertificateAuthority	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ACMPCA::CertificateAuthorityAtivação	Sim	Sim	Sim	Não
AWS::AccessAnalyzer::Analyzer	Sim	Sim	Sim	Não
AWS::AmazonMQ::Broker	Sim	Sim	Sim	Não
AWS::Amplify::App	Sim	Não	Nº	Nº
AWS::Amplify::Branch	Sim	Não	Nº	Nº
AWS::ApiGateway::RestApi	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ApiGateway::Stage	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Api	Sim	Sim	Sim	Sim
AWS::ApiGatewayV2::Stage	Sim	Sim	Sim	Sim
AWS::AppConfig::Application	Sim	Sim	Não	Sim
AWS::AppConfig::ConfigurationProfile	Sim	Sim	Não	Sim
AWS::AppConfig::DeploymentStrategy	Sim	Sim	Não	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::AppConfig::Environment	Sim	Sim	Não	Sim
AWS::AppConfig::ExtensionAssociation	Sim	Sim	Sim	Sim
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim	Não	Sim
AWS::AppIntegrations::EventIntegration	Não	Sim	Não	Nº
AWS::AppMesh::GatewayRoute	Sim	Sim	Não	Nº
AWS::AppMesh::Mesh	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::AppMesh::Route	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualGateway	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualNode	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualRouter	Sim	Sim	Não	Nº
AWS::AppMesh::VirtualService	Sim	Sim	Não	Nº
AWS::AppSync::GraphQLAPI	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Athena::DataCatalog	Sim	Sim	Sim	Não
AWS::Athena::PreparedStatement	Sim	Sim	Não	Nº
AWS::Athena::WorkGroup	Sim	Sim	Sim	Não
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim	Sim	Sim
AWS::AutoScaling::LaunchConfiguration	Sim	Sim	Sim	Sim
AWS::AutoScaling::ScalingPolicy	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::AutoScaling::ScheduledAction	Sim	Sim	Sim	Sim
AWS::AutoScaling::WarmPool	Sim	Sim	Não	Nº
AWS::Backup::BackupPlan	Sim	Sim	Não	Nº
AWS::Backup::BackupSelection	Sim	Sim	Sim	Não
AWS::Backup::BackupVault	Sim	Sim	Sim	Não
AWS::Backup::RecoveryPoint	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Backup::ReportPlan	Sim	Sim	Não	Nº
AWS::Batch::ComputeEnvironment	Sim	Sim	Sim	Não
AWS::Batch::JobQueue	Sim	Sim	Sim	Não
AWS::Batch::SchedulingPolicy	Sim	Sim	Sim	Não
AWS::Cassandra::Keyspace	Sim	Não	Nº	Nº
AWS::Cloud9::EnvironmentEC2	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::CloudFormation::Stack	Sim	Sim	Não	Nº
AWS::CloudTrail::Trail	Sim	Sim	Sim	Sim
AWS::CloudWatch::Alarm	Sim	Sim	Sim	Sim
AWS::CloudWatch::MetricStream	Sim	Sim	Sim	Sim
AWS::CodeBuild::Project	Sim	Sim	Sim	Sim
AWS::CodeBuild::ReportGroup	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::CodeDeploy::Application	Sim	Sim	Não	Nº
AWS::CodeDeploy::DeploymentConfig	Sim	Sim	Não	Nº
AWS::CodeDeploy::DeploymentGroup	Sim	Sim	Não	Nº
AWS::Cognito::UserPool	Sim	Não	Nº	Sim
AWS::Cognito::UserPoolCliente	Sim	Não	Nº	Sim
AWS::Cognito::UserPoolGrupo	Sim	Não	Nº	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Config::ConfigurationRecorder	Sim	Sim	Sim	Sim
AWS::Config::ConformancePackConformidade	Sim	Não	Nº	Nº
AWS::Config::ResourceCompliance	Sim	Sim	Sim	Sim
AWS::Connect::Instance	Não	Sim	Não	Nº
AWS::CustomerProfiles::Domain	Nº	Sim	Não	Nº
AWS::CustomerProfiles::ObjectType	Nº	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::DMS::Certificate	Sim	Sim	Não	Nº
AWS::DMS::Endpoint	Sim	Sim	Não	Nº
AWS::DMS::EventSubscription	Sim	Sim	Não	Nº
AWS::DMS::ReplicationInstance	Sim	Sim	Não	Nº
AWS::DMS::ReplicationSubnetGrupo	Sim	Sim	Não	Nº
AWS::DMS::ReplicationTask	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::DataSync::LocationEFS	Sim	Sim	Sim	Não
AWS::DataSync::LocationF SxLustre	Sim	Sim	Não	Nº
AWS::DataSync::LocationF SxWindows	Sim	Sim	Não	Nº
AWS::DataSync::LocationHDFS	Sim	Sim	Sim	Não
AWS::DataSync::LocationNFS	Sim	Sim	Sim	Não
AWS::DataSync::Loc ationObjectArmazenamento	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::DataSync::LocationS3	Sim	Sim	Sim	Não
AWS::DataSync::LocationSMB	Sim	Sim	Sim	Não
AWS::DataSync::Task	Sim	Sim	Sim	Não
AWS::Detective::Graph	Sim	Sim	Não	Nº
AWS::DynamoDB::Table	Sim	Sim	Sim	Sim
AWS::EC2::CapacityReservation	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::ClientVpnPonto final	Sim	Sim	Não	Nº
AWS::EC2::CustomerGateway	Sim	Sim	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim	Sim	Sim
AWS::EC2::EC2Fleet	Sim	Sim	Sim	Não
AWS::EC2::EIP	Sim	Sim	Sim	Sim
AWS::EC2::EgressOnlyInternetGateway	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::FlowLog	Sim	Sim	Sim	Não
AWS::EC2::Host	Sim	Sim	Sim	Sim
AWS::EC2::IPAM	Sim	Sim	Sim	Não
AWS::EC2::IPAMPool	Sim	Sim	Sim	Não
AWS::EC2::IPAMScope	Sim	Sim	Sim	Não
AWS::EC2::Instance	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::InternetGateway	Sim	Sim	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim	Não	Nº
AWS::EC2::NatGateway	Sim	Sim	Sim	Não
AWS::EC2::NetworkAcl	Sim	Sim	Sim	Sim
AWS::EC2::NetworkInsightsAccessScope	Sim	Sim	Não	Nº
AWS::EC2::NetworkI nsightsAccessScopeAnálise	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::NetworkInsightsAnálise	Sim	Sim	Não	Nº
AWS::EC2::NetworkInsightsCaminho	Sim	Sim	Não	Nº
AWS::EC2::NetworkInterface	Sim	Sim	Sim	Sim
AWS::EC2::PrefixList	Sim	Sim	Sim	Sim
AWS::EC2::RouteTable	Sim	Sim	Sim	Sim
AWS::EC2::SecurityGroup	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::SpotFleet	Sim	Sim	Sim	Sim
AWS::EC2::Subnet	Sim	Sim	Sim	Sim
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim	Sim	Sim
AWS::EC2::TrafficMirrorFiltrar	Sim	Não	Nº	Nº
AWS::EC2::TrafficMirrorSessão	Sim	Não	Nº	Nº
AWS::EC2::TrafficMirrorAlvo	Sim	Não	Nº	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::TransitGateway	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayAnexo	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayConnect	Sim	Sim	Sim	Não
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim	Sim	Sim
AWS::EC2::TransitGatewayRouteTable	Sim	Sim	Sim	Não
AWS::EC2::VPC	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EC2::VPCEndpoint	Sim	Sim	Sim	Sim
AWS: :EC2: :VPC EndpointService	Sim	Sim	Sim	Sim
AWS: :EC2: :VPC PeeringConnection	Sim	Sim	Sim	Sim
AWS::EC2::VPNConnection	Sim	Sim	Sim	Sim
AWS::EC2::VPNGateway	Sim	Sim	Sim	Sim
AWS::EC2::Volume	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ECR::PullThroughCacheRule	Sim	Sim	Sim	Sim
AWS::ECR::RegistryPolicy	Sim	Sim	Sim	Não
AWS::ECR::Repository	Sim	Sim	Sim	Não
AWS::ECS::CapacityProvider	Sim	Sim	Sim	Sim
AWS::ECS::Cluster	Sim	Sim	Sim	Sim
AWS::ECS::Service	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ECS::TaskDefinition	Sim	Sim	Sim	Sim
AWS::ECS::TaskSet	Sim	Sim	Sim	Não
AWS::EFS::AccessPoint	Sim	Sim	Sim	Não
AWS::EFS::FileSystem	Sim	Sim	Sim	Não
AWS::EKS::Addon	Sim	Sim	Sim	Não
AWS::EKS::Cluster	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::EKS::FargateProfile	Sim	Sim	Sim	Sim
AWS::EKS::IdentityProviderConfig	Sim	Sim	Sim	Não
AWS::EMR::SecurityConfiguration	Sim	Sim	Sim	Não
AWS::ElasticBeanstalk::Application	Nº	Sim	Não	Nº
AWS::ElasticBeanstalk::ApplicationVersion	Nº	Sim	Não	Nº
AWS::ElasticBeanstalk::Environment	Nº	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim	Sim	Sim
AWS::ElasticLoadBalancingV2::Listener	Sim	Sim	Não	Nº
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim	Sim	Sim
AWS::Elasticsearch::Domain	Sim	Sim	Sim	Sim
AWS::Events::ApiDestination	Sim	Sim	Não	Nº
AWS::Events::Archive	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Events::Connection	Sim	Sim	Não	Nº
AWS::Events::EventBus	Sim	Sim	Não	Nº
AWS::Events::Rule	Sim	Sim	Não	Nº
AWS::FIS::ExperimentTemplate	Sim	Sim	Não	Nº
AWS::Glue::Classifier	Sim	Sim	Sim	Sim
AWS::Glue::Job	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Glue: :Transformação de ML	Sim	Sim	Sim	Sim
AWS::GroundStation::Config	Sim	Sim	Não	Nº
AWS::GroundStation ::DataflowEndpointGrupo	Sim	Sim	Não	Nº
AWS::GroundStation::MissionProfile	Sim	Sim	Não	Nº
AWS::GuardDuty::Detector	Sim	Sim	Não	Nº
AWS::GuardDuty::Filter	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::GuardDever: :IPset	Sim	Sim	Não	Nº
AWS::GuardDuty::ThreatIntelConjunto	Sim	Sim	Não	Nº
AWS::IAM::Group	Sim	Sim	Não	Nº
AWS::IAM::Policy	Sim	Sim	Não	Nº
AWS::IAM::Role	Sim	Sim	Não	Nº
AWS::IAM::User	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ImageBuilder::ContainerRecipe	Sim	Sim	Sim	Sim
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim	Não	Nº
AWS::ImageBuilder::ImagePipeline	Sim	Sim	Sim	Sim
AWS::ImageBuilder::ImageRecipe	Sim	Sim	Não	Nº
AWS::ImageBuilder::InfrastructureConfiguration	Sim	Sim	Sim	Sim
AWS::InspectorV2::Filter	Sim	Não	Nº	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::IoT::AccountAuditConfiguração	Sim	Não	Sim	Não
AWS::IoT::Authorizer	Sim	Não	Sim	Não
AWS::IoCertificado T: :CA	Sim	Não	Sim	Não
AWS::IoT::CustomMetric	Sim	Não	Sim	Não
AWS::IoT::Dimension	Sim	Não	Sim	Não
AWS::IoT::FleetMetric	Sim	Não	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::IoT::JobTemplate	Sim	Não	Sim	Não
AWS::IoT::MitigationAction	Sim	Não	Sim	Não
AWS::IoT::Policy	Sim	Não	Sim	Não
AWS::IoT::ProvisioningTemplate	Sim	Não	Sim	Não
AWS::IoT::RoleAlias	Sim	Não	Sim	Não
AWS::IoT::ScheduledAudit	Sim	Não	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::IoT::SecurityProfile	Sim	Não	Sim	Não
AWS::KMS::Alias	Sim	Sim	Não	Nº
AWS::KMS::Key	Sim	Sim	Sim	Sim
AWS::Kinesis::Stream	Sim	Sim	Sim	Não
AWS::Kinesis::StreamConsumer	Sim	Sim	Sim	Não
AWS::KinesisAnalyticsV2::Application	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::KinesisFirehose::DeliveryStream	Sim	Sim	Sim	Sim
AWS::Lambda::CodeSigningConfig	Sim	Sim	Não	Nº
AWS::Lambda::Function	Sim	Sim	Sim	Sim
AWS::Lex::Bot	Não	Sim	Não	Nº
AWS::Lex::BotAlias	Nº	Sim	Não	Nº
AWS::Logs::Destination	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::MSK::BatchScramSegredo	Sim	Sim	Sim	Não
AWS::MSK::Cluster	Sim	Sim	Sim	Não
AWS::MSK::ClusterPolicy	Sim	Sim	Sim	Sim
AWS::MSK::Configuration	Sim	Sim	Sim	Não
AWS::MSK::VpcConnection	Sim	Sim	Sim	Sim
AWS::MediaConnect::FlowEntitlement	Não	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::MediaConnect::FlowSource	Nº	Sim	Não	Nº
AWS::MediaConnect::FlowVpcInterface	Nº	Sim	Não	Nº
AWS::MediaTailor::PlaybackConfiguration	Nº	Sim	Não	Nº
AWS::NetworkFirewall::Firewall	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim	Sim	Sim
AWS::NetworkFirewall::RuleGroup	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::NetworkFirewall: :TLS InspectionConfiguration	Sim	Sim	Sim	Sim
AWS::OpenSearch::Domain	Sim	Sim	Não	Nº
AWS::RDS::DBCluster	Sim	Sim	Sim	Não
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim	Sim	Não
AWS::RDS::DBInstance	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SecurityGroup	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::RDS::DBSnapshot	Sim	Sim	Sim	Sim
AWS: :RDS: :DB SubnetGroup	Sim	Sim	Sim	Sim
AWS::RDS::EventSubscription	Sim	Sim	Sim	Sim
AWS::RDS::OptionGroup	Sim	Sim	Sim	Não
AWS::Redshift::Cluster	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterParameterGrupo	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSnapshot	Sim	Sim	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim	Sim	Sim
AWS::Redshift::EventSubscription	Sim	Sim	Sim	Sim
AWS::Redshift::ScheduledAction	Sim	Não	Nº	Nº
AWS::ResilienceHub::App	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ResilienceHub::ResiliencyPolicy	Sim	Sim	Não	Nº
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim	Não	Nº
AWS::Route53Resolver::FirewallRuleGrupo	Sim	Sim	Não	Nº
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim	Não	Nº
AWS::Route53Resolver::ResolverEndpoint	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Sim	Não	Nº
AWS::Route53Resolver::ResolverRule	Sim	Sim	Sim	Não
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Sim	Sim	Não
AWS::S3::AccessPoint	Sim	Sim	Sim	Sim
AWS::S3::AccountPublicAccessBlock	Sim	Sim	Não	Nº
AWS::S3::Bucket	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::SES::ConfigurationSet	Sim	Sim	Não	Nº
AWS::SES::ContactList	Sim	Sim	Não	Nº
AWS::SES::Template	Sim	Sim	Não	Nº
AWS::SNS::Topic	Sim	Sim	Não	Nº
AWS::SQS::Queue	Sim	Sim	Não	Nº
AWS::SSM::AssociationCompliance	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::SSM::Document	Sim	Sim	Sim	Sim
AWS::SSM::FileData	Sim	Sim	Sim	Sim
AWS::SSM::ManagedInstanceInventário	Sim	Sim	Sim	Sim
AWS::SSM::PatchCompliance	Sim	Sim	Sim	Sim
AWS::SageMaker::AppImageConfig	Sim	Sim	Não	Nº
AWS::SageMaker::CodeRepository	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::SageMaker::Domain	Sim	Sim	Não	Nº
AWS::SageMaker::EndpointConfig	Sim	Sim	Não	Nº
AWS::SageMaker::FeatureGroup	Sim	Sim	Não	Nº
AWS::SageMaker::Image	Sim	Sim	Não	Nº
AWS::SageMaker::Model	Sim	Sim	Não	Nº
AWS::SageMaker::NotebookInstance	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Sim	Sim	Não	Nº
AWS::SecretsManager::Secret	Sim	Sim	Sim	Sim
AWS::ServiceCatalog::CloudFormationProduto	Sim	Sim	Sim	Não
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Sim	Sim	Não
AWS::ServiceCatalog::Portfolio	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::HttpNamespace	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::ServiceDiscovery::Instance	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::PublicDnsNamespace	Sim	Sim	Sim	Não
AWS::ServiceDiscovery::Service	Sim	Sim	Sim	Não
AWS::ShieldRegional::Protection	Sim	Sim	Sim	Não
AWS::Signer::SigningProfile	Sim	Sim	Não	Nº
AWS::StepFunctions::Activity	Sim	Sim	Sim	Não

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::StepFunctions::StateMachine	Sim	Sim	Sim	Não
AWS::Transfer::Agreement	Sim	Sim	Sim	Não
AWS::Transfer::Certificate	Sim	Sim	Sim	Não
AWS::Transfer::Connector	Sim	Sim	Sim	Não
AWS::Transfer::Profile	Sim	Sim	Sim	Sim
AWS::Transfer::Workflow	Sim	Sim	Não	Nº

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::WAFRegional::RateBasedRegra	Sim	Sim	Sim	Sim
AWS::WAFRegional::Rule	Sim	Sim	Sim	Sim
AWS::WAFRegional::RuleGroup	Sim	Sim	Sim	Sim
AWS::WAFRegional::WebACL	Sim	Sim	Sim	Sim
AWS::WAFv2::IPSet	Sim	Sim	Sim	Sim
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim	Sim	Sim

Tipo de atributo	África (Cidade do Cabo)	Oriente Médio (Bahrein)	Oriente Médio (Emirados Árabes Unidos)	Israel (Tel Aviv)
AWS::WAFv2::RegexPatternConjunto	Sim	Sim	Sim	Sim
AWS::WAFv2::RuleGroup	Sim	Sim	Sim	Sim
AWS::WAFv2::WebACL	Sim	Sim	Sim	Sim
AWS::WorkSpaces::Workspace	Não	Sim	Não	Nº
AWS::XRay::EncryptionConfig	Nº	Sim	Sim	Sim

GovCloud Regiões

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::ACM::Certificate	Sim	Sim
AWS::ACMPCA::CertificateAuthority	Sim	Sim
AWS::ACMPCA::CertificateAuthorityAtivação	Sim	Sim
AWS::AccessAnalyzer::Analyzer	Sim	Sim
AWS::AmazonMQ::Broker	Sim	Sim
AWS::ApiGateway::RestApi	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::ApiGateway::Stage	Sim	Sim
AWS::ApiGatewayV2::Api	Sim	Sim
AWS::ApiGatewayV2::Stage	Sim	Sim
AWS::AppConfig::Application	Sim	Sim
AWS::AppConfig::ConfigurationProfile	Sim	Sim
AWS::AppConfig::DeploymentStrategy	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::AppConfig::Environment	Sim	Sim
AWS::AppConfig::ExtensionAssociation	Sim	Sim
AWS::AppConfig::HostedConfigurationVersão	Sim	Sim
AWS::AppStream::Application	Sim	Sim
AWS::AppStream::DirectoryConfig	Não	Sim
AWS::AppStream::Fleet	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::AppStream::Stack	Não	Sim
AWS::Athena::DataCatalog	Sim	Sim
AWS::Athena::WorkGroup	Sim	Sim
AWS::AutoScaling::AutoScalingGrupo	Sim	Sim
AWS::AutoScaling::LaunchConfiguration	Sim	Sim
AWS::AutoScaling::ScalingPolicy	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::AutoScaling::ScheduledAction	Sim	Sim
AWS::AutoScaling::WarmPool	Sim	Sim
AWS::Backup::BackupPlan	Sim	Sim
AWS::Backup::BackupSelection	Sim	Sim
AWS::Backup::BackupVault	Sim	Sim
AWS::Backup::RecoveryPoint	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Batch::ComputeEnvironment	Sim	Sim
AWS::Batch::JobQueue	Sim	Sim
AWS::Batch::SchedulingPolicy	Sim	Sim
AWS::Cassandra::Keyspace	Sim	Sim
AWS::CloudFormation::Stack	Sim	Sim
AWS::CloudTrail::Trail	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::CloudWatch::Alarm	Sim	Sim
AWS::CodeBuild::Project	Sim	Sim
AWS::CodeBuild::ReportGroup	Sim	Sim
AWS::Cognito::UserPoolGrupo	Nº	Sim
AWS::Config::ConfigurationRecorder	Sim	Sim
AWS::Config::ConformancePackConformidade	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Config::ResourceCompliance	Sim	Sim
AWS::Connect::Instance	Não	Sim
AWS::Connect::QuickConnect	Não	Sim
AWS::DMS::Certificate	Sim	Sim
AWS::DMS::Endpoint	Sim	Sim
AWS::DMS::EventSubscription	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::DMS::ReplicationInstance	Sim	Sim
AWS::DMS::ReplicationSubnetGrupo	Sim	Sim
AWS::DMS::ReplicationTask	Sim	Sim
AWS::DataSync::LocationEFS	Sim	Sim
AWS::DataSync::LocationF SxLustre	Sim	Sim
AWS::DataSync::LocationF SxWindows	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::DataSync::LocationHDFS	Sim	Sim
AWS::DataSync::LocationNFS	Sim	Sim
AWS::DataSync::LocationObjectArmazenamento	Sim	Sim
AWS::DataSync::LocationS3	Sim	Sim
AWS::DataSync::LocationSMB	Sim	Sim
AWS::DataSync::Task	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Detective::Graph	Sim	Sim
AWS::DynamoDB::Table	Sim	Sim
AWS::EC2::CapacityReservation	Sim	Sim
AWS::EC2::ClientVpnPonto final	Sim	Sim
AWS::EC2::CustomerGateway	Sim	Sim
AWS::EC2::DHCPOptions	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EC2::EC2Fleet	Sim	Sim
AWS::EC2::EIP	Sim	Sim
AWS::EC2::EgressOnlyInternetGateway	Sim	Sim
AWS::EC2::FlowLog	Sim	Sim
AWS::EC2::Host	Sim	Sim
AWS::EC2::IPAM	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EC2::IPAMPool	Sim	Sim
AWS::EC2::IPAMScope	Sim	Sim
AWS::EC2::Instance	Sim	Sim
AWS::EC2::InternetGateway	Sim	Sim
AWS::EC2::LaunchTemplate	Sim	Sim
AWS::EC2::NatGateway	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EC2::NetworkAcl	Sim	Sim
AWS::EC2::NetworkInterface	Sim	Sim
AWS::EC2::PrefixList	Sim	Sim
AWS::EC2::RouteTable	Sim	Sim
AWS::EC2::SecurityGroup	Sim	Sim
AWS::EC2::SpotFleet	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EC2::Subnet	Sim	Sim
AWS::EC2::SubnetRouteTableAssociation	Sim	Sim
AWS::EC2::TrafficMirrorFiltrar	Sim	Sim
AWS::EC2::TrafficMirrorSessão	Sim	Sim
AWS::EC2::TrafficMirrorAlvo	Sim	Sim
AWS::EC2::TransitGateway	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EC2::TransitGatewayAnexo	Sim	Sim
AWS::EC2::TransitGatewayConnect	Sim	Sim
AWS::EC2::TransitGatewayMulticastDomain	Sim	Sim
AWS::EC2::TransitGatewayRouteTable	Sim	Sim
AWS::EC2::VPC	Sim	Sim
AWS::EC2::VPCEndpoint	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS: :EC2: :VPC EndpointService	Nº	Sim
AWS: :EC2: :VPC PeeringConnection	Sim	Sim
AWS::EC2::VPNConnection	Sim	Sim
AWS::EC2::VPNGateway	Sim	Sim
AWS::EC2::Volume	Sim	Sim
AWS::ECR::Repository	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::ECS::CapacityProvider	Sim	Sim
AWS::ECS::Cluster	Sim	Sim
AWS::ECS::Service	Sim	Sim
AWS::ECS::TaskDefinition	Sim	Sim
AWS::ECS::TaskSet	Sim	Sim
AWS::EFS::AccessPoint	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::EFS::FileSystem	Sim	Sim
AWS::EKS::Addon	Sim	Sim
AWS::EKS::Cluster	Sim	Sim
AWS::EKS::IdentityProviderConfig	Sim	Sim
AWS::EMR::SecurityConfiguration	Sim	Sim
AWS::ElasticBeanstalk::Application	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::ElasticBeanstalk::ApplicationVersion	Sim	Sim
AWS::ElasticBeanstalk::Environment	Sim	Sim
AWS::ElasticLoadBalancing::LoadBalancer	Sim	Sim
AWS::ElasticLoadBalancingV2::Listener	Sim	Sim
AWS::ElasticLoadBalancingV2::LoadBalancer	Sim	Sim
AWS::Elasticsearch::Domain	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Events::EventBus	Sim	Sim
AWS::Events::Rule	Sim	Sim
AWS::FIS::ExperimentTemplate	Sim	Sim
AWS::Glue::Classifier	Sim	Sim
AWS::Glue::Job	Sim	Sim
AWS::Glue: :Transformação de ML	Nº	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::GreengrassV2::ComponentVersion	Sim	Sim
AWS::GuardDuty::Detector	Sim	Sim
AWS::GuardDuty::Filter	Sim	Sim
AWS::GuardDever: :IPset	Sim	Sim
AWS::GuardDuty::ThreatIntelConjunto	Sim	Sim
AWS::IAM::Group	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IAM::InstanceProfile	Sim	Não
AWS::IAM::OIDCProvider	Sim	Não
AWS::IAM::Policy	Sim	Sim
AWS::IAM::Role	Sim	Sim
AWS::IAM::SAMLProvider	Sim	Não
AWS::IAM::ServerCertificate	Sim	Não

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IAM::User	Sim	Sim
AWS::ImageBuilder::ContainerRecipe	Sim	Sim
AWS::ImageBuilder::DistributionConfiguration	Sim	Sim
AWS::ImageBuilder::ImagePipeline	Sim	Sim
AWS::ImageBuilder::ImageRecipe	Sim	Sim
AWS::ImageBuilder::InfrastructureConfiguration	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IoT::AccountAuditConfiguração	Sim	Sim
AWS::IoT::Authorizer	Sim	Sim
AWS::IoCertificado T: :CA	Sim	Sim
AWS::IoT::CustomMetric	Sim	Sim
AWS::IoT::Dimension	Sim	Sim
AWS::IoT::FleetMetric	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IoT::JobTemplate	Sim	Sim
AWS::IoT::MitigationAction	Sim	Sim
AWS::IoT::Policy	Sim	Sim
AWS::IoT::ProvisioningTemplate	Sim	Sim
AWS::IoT::RoleAlias	Sim	Sim
AWS::IoT::ScheduledAudit	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IoT::SecurityProfile	Sim	Sim
AWS::IoTEvents::AlarmModel	Não	Sim
AWS::IoTEvents::DetectorModel	Não	Sim
AWS::IoTEvents::Input	Não	Sim
AWS::IoTSiteWise::AssetModel	Não	Sim
AWS::IoTSiteWise::Gateway	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::IoTSiteWise::Portal	Não	Sim
AWS::IoTTwinMaker::ComponentType	Não	Sim
AWS::IoTTwinMaker::Entity	Não	Sim
AWS::IoTTwinMaker::Workspace	Não	Sim
AWS::KMS::Alias	Sim	Sim
AWS::KMS::Key	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Kinesis::Stream	Sim	Sim
AWS::Kinesis::StreamConsumer	Sim	Sim
AWS::KinesisAnalyticsV2::Application	Sim	Sim
AWS::KinesisFirehose::DeliveryStream	Sim	Sim
AWS::Lambda::Function	Sim	Sim
AWS::Logs::Destination	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::MSK::BatchScramSegredo	Sim	Sim
AWS::MSK::Cluster	Sim	Sim
AWS::MSK::ClusterPolicy	Sim	Sim
AWS::MSK::Configuration	Sim	Sim
AWS::MSK::VpcConnection	Sim	Sim
AWS::NetworkFirewall::Firewall	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::NetworkFirewall::FirewallPolicy	Sim	Sim
AWS::NetworkFirewall::RuleGroup	Sim	Sim
AWS::NetworkManager::CustomerGatewayAssociação	Nº	Sim
AWS::NetworkManager::Device	Não	Sim
AWS::NetworkManager::GlobalNetwork	Não	Sim
AWS::NetworkManager::Link	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::NetworkManager::LinkAssociation	Não	Sim
AWS::NetworkManager::Site	Não	Sim
AWS::NetworkManager::TransitGatewayRegistro	Nº	Sim
AWS::OpenSearch::Domain	Sim	Sim
AWS::Pinpoint::App	Não	Sim
AWS::Pinpoint::ApplicationSettings	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Pinpoint::Campaign	Não	Sim
AWS::Pinpoint::EmailChannel	Não	Sim
AWS::Pinpoint::EmailTemplate	Não	Sim
AWS::Pinpoint::EventStream	Não	Sim
AWS::Pinpoint::InAppModelo	Nº	Sim
AWS::Pinpoint::Segment	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::QuickSight::Template	Não	Sim
AWS::RDS::DBCluster	Sim	Sim
AWS: :RDS: :DB ClusterSnapshot	Sim	Sim
AWS::RDS::DBInstance	Sim	Sim
AWS: :RDS: :DB SecurityGroup	Sim	Sim
AWS::RDS::DBSnapshot	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS: :RDS: :DB SubnetGroup	Sim	Sim
AWS::RDS::EventSubscription	Sim	Sim
AWS::RDS::OptionGroup	Sim	Sim
AWS::Redshift::Cluster	Sim	Sim
AWS::Redshift::ClusterParameterGrupo	Sim	Sim
AWS::Redshift::ClusterSecurityGrupo	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Redshift::ClusterSnapshot	Sim	Sim
AWS::Redshift::ClusterSubnetGrupo	Sim	Sim
AWS::Redshift::EventSubscription	Sim	Sim
AWS::Redshift::ScheduledAction	Sim	Sim
AWS::RoboMaker::RobotApplication	Não	Sim
AWS::RoboMaker::RobotApplicationVersão	Nº	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::RoboMaker::SimulationApplication	Não	Sim
AWS::Route53Resolver::FirewallDomainLista	Sim	Sim
AWS::Route53Resolver::FirewallRuleGrupo	Sim	Sim
AWS::Route53Resolver::FirewallRuleGroupAssociation	Sim	Sim
AWS::Route53Resolver::ResolverEndpoint	Sim	Sim
AWS::Route53Resolver::ResolverQueryLoggingConfig	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociação	Sim	Sim
AWS::Route53Resolver::ResolverRule	Sim	Sim
AWS::Route53Resolver::ResolverRuleAssociação	Sim	Sim
AWS::S3::AccessPoint	Sim	Sim
AWS::S3::AccountPublicAccessBlock	Sim	Sim
AWS::S3::Bucket	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::SES::ConfigurationSet	Não	Sim
AWS::SES::ContactList	Não	Sim
AWS::SES::Template	Não	Sim
AWS::SNS::Topic	Sim	Sim
AWS::SQS::Queue	Sim	Sim
AWS::SSM::AssociationCompliance	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::SSM::Document	Sim	Sim
AWS::SSM::FileData	Sim	Sim
AWS::SSM::ManagedInstanceInventário	Sim	Sim
AWS::SSM::PatchCompliance	Sim	Sim
AWS::SageMaker::Model	Não	Sim
AWS::SageMaker::NotebookInstance	Não	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::SageMaker::NotebookInstanceLifecycleConfig	Não	Sim
AWS::SecretsManager::Secret	Sim	Sim
AWS::ServiceCatalog::CloudFormationProduto	Sim	Sim
AWS::ServiceCatalog::CloudFormationProvisionedProduct	Sim	Sim
AWS::ServiceCatalog::Portfolio	Sim	Sim
AWS::ServiceDiscovery::HttpNamespace	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::ServiceDiscovery::Instance	Sim	Sim
AWS::ServiceDiscovery::Service	Sim	Sim
AWS::StepFunctions::StateMachine	Sim	Sim
AWS::Transfer::Agreement	Sim	Sim
AWS::Transfer::Certificate	Sim	Sim
AWS::Transfer::Connector	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::Transfer::Profile	Sim	Sim
AWS::Transfer::Workflow	Sim	Sim
AWS::WAFRegional::RateBasedRegra	Sim	Sim
AWS::WAFRegional::Rule	Sim	Sim
AWS::WAFRegional::RuleGroup	Sim	Sim
AWS::WAFRegional::WebACL	Sim	Sim

Tipo de atributo	AWS GovCloud (Oeste dos EUA)	AWS GovCloud (Leste dos EUA)
AWS::WAFv2::IPSet	Sim	Sim
AWS::WAFv2::ManagedRuleConjunto	Sim	Sim
AWS::WAFv2::RegexPatternConjunto	Sim	Sim
AWS::WAFv2::RuleGroup	Sim	Sim
AWS::WAFv2::WebACL	Sim	Sim
AWS::WorkSpaces::Workspace	Não	Sim

AWS Recursos de gravação

AWS Config detecta continuamente quando os tipos de recursos compatíveis são criados, alterados ou excluídos. AWS Config registra esses eventos como itens de configuração (CIs). Você pode personalizar o AWS Config para registrar as alterações para todos os tipos de recursos compatíveis ou apenas para os tipos que são relevantes para você. Para obter uma lista dos tipos de recursos compatíveis que AWS Config podem gravar, consulteTipos de recursos compatíveis.

Considerações

Alto número de AWS Config avaliações

Você pode notar um aumento na atividade em sua conta durante a gravação do mês inicial com o AWS Config em comparação com os meses subsequentes. Durante o processo inicial de inicialização, AWS Config executa avaliações em todos os recursos da sua conta que você selecionou para serem registrados. AWS Config

Se você estiver executando cargas de trabalho efêmeras, poderá observar um aumento na atividade ao registrar AWS Config as alterações de configuração associadas à criação e exclusão desses recursos temporários. Um workload efêmero é um uso temporário de recursos de computação que são carregados e executados quando necessário. Exemplos incluem instâncias spot do Amazon Elastic Compute Cloud (Amazon EC2), trabalhos do Amazon EMR e o AWS Auto Scaling. Se quiser evitar o aumento da atividade decorrente da execução de cargas de trabalho efêmeras, você pode configurar o gravador de configuração para excluir esses tipos de recursos do registro ou executar esses tipos de cargas de trabalho em uma conta separada, AWS Config desativada, para evitar maiores registros de configuração e avaliações de regras.

Disponibilidade de regiões

Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você AWS Config configurou. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você configurou AWS Config.

Quais são as diferenças entre recursos regionais e globais?

Recursos regionais

Os recursos regionais estão vinculados a uma região e somente podem ser usados naquela região. Você os cria em um determinado local e Região da AWS, em seguida, eles existem nessa região. Para ver ou interagir com esses recursos, você deve direcionar suas operações para essa região. Por exemplo, para criar uma instância do Amazon EC2 com o AWS Management Console, você escolhe Região da AWS aquela na qual deseja criar a instância. Se você usar o AWS Command Line Interface (AWS CLI) para criar a instância, inclua o `--region` parâmetro. Cada um dos AWS SDKs tem seu próprio mecanismo equivalente para especificar a região que a operação usa.

Há vários motivos para usar recursos regionais. Um dos motivos é garantir que os recursos e os endpoints de serviço que você usa para acessá-los estejam o mais próximos possível do cliente. Isso melhora a performance ao minimizar a latência. Outro motivo é fornecer um limite de isolamento. Isso permite criar cópias independentes de recursos em várias regiões para distribuir a carga e melhorar a escalabilidade. Ao mesmo tempo, ele isola os recursos uns dos outros para melhorar a disponibilidade.

Se você especificar um diferente Região da AWS no console ou em um AWS CLI comando, não poderá mais ver ou interagir com os recursos que podia ver na região anterior.

Quando você analisa o nome do recurso da Amazon (ARN) de um recurso regional, a região que contém o recurso é especificada como o quarto campo no ARN. Por exemplo, uma instância do Amazon EC2 é um recurso regional. Este é um exemplo de um ARN para uma instância do Amazon EC2 que existe na região `us-east-1`.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Recursos globais

Alguns recursos de AWS serviços são recursos globais, o que significa que você pode usar o recurso de qualquer lugar. Você não especifica uma Região da AWS no console de um serviço global. Para acessar um recurso global, você não especifica um `--region` parâmetro ao usar as operações do serviço AWS CLI e do AWS SDK.

Os recursos globais oferecem suporte a casos em que é fundamental que somente uma instância de um recurso específico possa existir por vez. Nesses cenários, a replicação ou sincronização entre cópias em diferentes regiões não é adequada. Ter que acessar um único endpoint global,

com o possível aumento na latência, é considerado aceitável para garantir que quaisquer alterações sejam instantaneamente visíveis para os consumidores do recurso.

Por exemplo, os clusters globais do Amazon Aurora (`AWS::RDS::GlobalCluster`) são recursos globais e, portanto, não estão vinculados a uma região. Isso significa que você pode criar um cluster global sem depender de um endpoint regional. A vantagem é que, embora o Amazon Relational Database Service (Amazon RDS) em si seja organizado por regiões, a região específica de origem de um cluster global não afeta o cluster global. Ele aparece como um cluster global único e contínuo em todas as regiões.

O nome do recurso da Amazon (ARN) de um recurso global não inclui uma região. O quarto campo está vazio, como no exemplo a seguir de um ARN para um cluster global.

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> Os tipos de recursos globais integrados AWS Config após fevereiro de 2022 serão registrados somente na região de origem do serviço para a partição comercial e AWS GovCloud (Oeste dos EUA) para a partição. GovCloud Você pode visualizar os itens de configuração (CIs) desses novos tipos de recursos globais somente em sua região de origem e AWS GovCloud (Oeste dos EUA).
> Os tipos de recursos globais integrados antes de fevereiro de 2022 (`AWS::IAM::Group`, `AWS::IAM::Policy`, `AWS::IAM::Role` e `AWS::IAM::User`) permanecem inalterados. Você pode ativar o registro desses recursos globais do IAM em todas as regiões em que AWS Config havia suporte antes de fevereiro de 2022. Esses recursos globais do IAM não podem ser registrados em regiões com suporte AWS Config após fevereiro de 2022.

Tipos de recursos globais | Recursos do IAM

Os seguintes tipos de recursos do IAM também são recursos globais: usuários, grupos, perfis do IAM e políticas gerenciadas pelo cliente. Esses tipos de recursos podem ser registrados nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Para evitar itens de configuração (CIs) duplicados, considere registrar somente os tipos de recursos globais do IAM uma vez em uma das regiões compatíveis. Isso também pode ajudar a evitar avaliações desnecessárias e controle de utilização da API.

Tipos de recursos globais | Somente na região de origem

Os recursos globais para os seguintes serviços são registrados somente AWS Config na região de origem do tipo de recurso global: Amazon Elastic Container Registry Public AWS Global Accelerator, Amazon Route 53 CloudFront, Amazon AWS WAF e. Para esses recursos globais, a mesma instância do tipo de recurso pode ser usada em várias AWS regiões, mas os itens de configuração (CIs) são registrados somente na região de origem da partição comercial ou AWS GovCloud (Oeste dos EUA) da AWS GovCloud (US) partição.

Regiões de origem para tipos de recursos globais

AWS Serviço	Valor de tipo de recurso	Região inicial
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	Região Leste dos EUA (N. da Virgínia)
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	Região Oeste dos EUA (Oregon)
	`AWS::GlobalAccelerator::EndpointGroup`	Região Oeste dos EUA (Oregon)
	`AWS::GlobalAccelerator::Accelerator`	Região Oeste dos EUA (Oregon)
Amazon Route 53	`AWS::Route53::HostedZone`	Região Leste dos EUA (N. da Virgínia)
	`AWS::Route53::HealthCheck`	Região Leste dos EUA (N. da Virgínia)
Amazon CloudFront	`AWS::CloudFront::Distribution`	Região Leste dos EUA (N. da Virgínia)
AWS WAF	`AWS::WAFv2::WebACL`	Região Leste dos EUA (N. da Virgínia)

Tipos de recursos globais | Clusters globais do Aurora

`AWS::RDS::GlobalClusteré` um recurso global que é registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado. Esse tipo de recurso global é exclusivo, pois se você habilitar o registro desse recurso em uma região, AWS Config registrará itens de configuração (CIs) desse tipo de recurso em todas as regiões habilitadas.

Se você não quiser gravar `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, use uma das seguintes estratégias de gravação para o AWS Config console:

- Grave todos os tipos de recursos com substituições personalizáveis, escolha "AWS RDS GlobalCluster “e escolha a substituição “Excluir da gravação”
- Registrar tipos de recursos específicos

Se você não quiser gravar o `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, use uma das seguintes estratégias de gravação para a API/CLI:

- Gravar todos os tipos de recursos atuais e futuros com exclusões (`EXCLUSION_BY_RESOURCE_TYPES`)
- Registrar tipos de recursos específicos (`INCLUSION_BY_RESOURCE_TYPES`)

Recursos de gravação no AWS Config console

Gravar recursos (console)

Você pode usar o AWS Config console para selecionar os tipos de recursos que AWS Config registra.

Para selecionar recursos

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configurações no painel de configuração à esquerda e, depois, escolha Editar. Para obter a lista de regiões compatíveis, consulte Endpoints e cotas do AWS Config no Referência geral da Amazon Web Services.
3. Na seção Método de gravação, selecione uma estratégia de gravação. Você pode especificar os AWS recursos que AWS Config deseja registrar.

All resource types with customizable overrides

Configure AWS Config para registrar as alterações de configuração para todos os tipos de recursos suportados atuais e futuros nesta região. É possível substituir a frequência de gravação ou excluir tipos de recursos específicos da gravação. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

- Configurações padrão

  Configure a frequência de gravação padrão para todos os tipos de recursos compatíveis atuais e futuros. Para obter mais informações, consulte Frequência de gravação.

  - Gravação contínua — AWS Config registrará as alterações de configuração continuamente sempre que uma alteração ocorrer.
  - Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior registrado.

  > **Note**
  >
  > AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- Configurações de substituição

  Substitua a frequência de gravação ou exclua tipos de recursos específicos da gravação. Se você selecionar a frequência de gravação ou interromper a gravação de um tipo de recurso, os itens de configuração já gravados permanecerão inalterados.

  > **Note**
  >
  > Tipos de recursos globais | Os clusters globais do Aurora são inicialmente incluídos na gravação
  >
  > O tipo de `AWS::RDS::GlobalCluster` recurso será registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado.

Se você não quiser gravar o `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, selecione “AWS RDS GlobalCluster” e escolha a substituição “Excluir da gravação”.

> **Note**
>
> Tipos de recursos globais | Os tipos de recursos do IAM são inicialmente excluídos da gravação
>
> “Todos os tipos de recursos do IAM gravados globalmente” são inicialmente excluídos da gravação para ajudar a reduzir custos. Esse pacote inclui usuários, grupos e perfis do IAM e políticas gerenciadas pelo cliente. Selecione Remover para remover a substituição e incluir esses recursos na gravação.
>
> A exceção a essa observação refere-se à região do Leste dos EUA (Norte da Virgínia). Os tipos de recursos globais do IAM são inicialmente incluídos na região do Leste dos EUA (Norte da Virgínia), pois essa região funciona como a origem dos tipos de recursos globais do IAM.
>
> Além disso, os tipos globais de recursos do IAM (`AWS::IAM::UserAWS::IAM::Group`,`AWS::IAM::Role`, e`AWS::IAM::Policy`) não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

> **Note**
>
> Limites
>
> É possível adicionar até cem substituições de frequência e seiscentas substituições de exclusão.
>
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Specific resource types

Configure AWS Config para registrar as alterações de configuração somente para os tipos de recursos que você especificar.

- Tipos de recursos específicos

  Selecione um tipo de recurso a ser gravado e a frequência. Para obter mais informações, consulte Frequência de gravação.

  - Gravação contínua — AWS Config registrará as alterações de configuração continuamente sempre que uma alteração ocorrer.
  - Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior registrado.

  > **Note**
  >
  > AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

  Se você selecionar a frequência de gravação ou interromper a gravação de um tipo de recurso, os itens de configuração já gravados permanecerão inalterados.

> **Note**
>
> Disponibilidade de regiões
> Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você AWS Config configurou. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você configurou AWS Config.

> **Note**
>
> Limites
>
> Não haverá limites se todos os tipos de recursos tiverem a mesma frequência. Será possível adicionar até cem tipos de recursos com frequência diária se pelo menos um tipo de recurso estiver definido como Contínua.
>
> A frequência diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

4. Escolha Salvar para salvar as alterações.

Recursos de gravação com a AWS CLI

Recursos de gravação (AWS CLI)

Você pode usar a AWS CLI para selecionar os tipos de recursos que deseja AWS Config registrar. Isso é feito por meio da criação de um gravador de configuração, que registra os tipos de recursos que você especifica em um grupo de registro. No grupo de registro, é necessário especificar se todos os tipos de recursos compatíveis ou somente tipos específicos de recursos são registrados.

Record all current and future supported resource types

Configure AWS Config para registrar as alterações de configuração para todos os tipos de recursos suportados atuais e futuros nesta região. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

1. Use o seguinte comando `put-configuration-recorder`:

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

Esse comando usa `--configuration-recorder` os `---recording-group` campos e.

> **Note**
>
> Grupo de gravação e gravador de configuração
> O campo `--recording-group` especifica quais tipos de recursos são gravados. O `--configuration-recorder` campo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

i. O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--recording-group`:

- `allSupported=true`— AWS Config registra as alterações na configuração de todos os tipos de recursos compatíveis, excluindo os tipos globais de recursos do IAM. Quando AWS Config adiciona suporte para um novo tipo de recurso, AWS Config começa a gravar recursos desse tipo automaticamente.
- `includeGlobalResourceTypes=true`: essa opção é um pacote que se aplica apenas aos tipos globais de recursos do IAM: usuários, grupos, perfis e políticas gerenciadas pelo cliente do IAM. Esses tipos de recursos globais do IAM só podem ser registrados AWS Config em regiões onde AWS Config estavam disponíveis antes de fevereiro de 2022. Você não pode registrar os tipos de recursos globais do IAM nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

> **Important**
>
> Os clusters globais do Aurora são gravados em todas as regiões habilitadas
> O tipo de `AWS::RDS::GlobalCluster` recurso será registrado em todas as AWS Config regiões suportadas nas quais o gravador de configuração está ativado, mesmo que não `includeGlobalResourceTypes` esteja definido como. `true` A opção `includeGlobalResourceTypes` é um pacote que se aplica apenas a usuários, grupos e perfis do IAM, além de políticas gerenciadas pelo cliente.
> Se você não quiser registrar `AWS::RDS::GlobalCluster` em todas as regiões habilitadas, use uma das seguintes estratégias de registro:

1. Gravar todos os tipos de recurso atuais e futuros excluindo os tipos especificados (`EXCLUSION_BY_RESOURCE_TYPES`) ou
2. Registrar tipos de recursos específicos (`INCLUSION_BY_RESOURCE_TYPES`)

Para obter mais informações, consulte Selecting Which Resources are Recorded | Regional and Global Resources.

> **Important**
>
> inclusão GlobalResourceTypes e a estratégia de registro de exclusão
> O `includeGlobalResourceTypes` campo não tem impacto na estratégia `EXCLUSION_BY_RESOURCE_TYPES` de gravação. Isso significa que os tipos globais de recursos do IAM (usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM) não serão adicionados automaticamente como exclusões de `exclusionByResourceTypes` quando `includeGlobalResourceTypes` estiver definido como. `false`
> O `includeGlobalResourceTypes` campo só deve ser usado para modificar o `AllSupported` campo, pois o padrão para o `AllSupported` campo é registrar as alterações de configuração para todos os tipos de recursos compatíveis, exceto os tipos de recursos globais do IAM. Para incluir os tipos de recursos globais do IAM quando `AllSupported` estiver definido como`true`, certifique-se de `includeGlobalResourceTypes` definir como`true`.
> Para excluir os tipos de recursos globais do IAM para a estratégia de `EXCLUSION_BY_RESOURCE_TYPES` gravação, você precisa adicioná-los manualmente ao `resourceTypes` campo de`exclusionByResourceTypes`.

> **Note**
>
> Campos obrigatórios e opcionais
> Para definir `includeGlobalResourceTypes` como `true`, defina o campo `allSupported` como `true`.
> Também há a opção de definir o campo `useOnly` de `RecordingStrategy` como `ALL_SUPPORTED_RESOURCE_TYPES`.

> **Note**
>
> Campos de substituição
>
> Se você `includeGlobalResourceTypes` definir como`false`, mas listar os tipos globais de recursos do IAM no `resourceTypes` campo de RecordingGroup, ainda AWS Config registrará as alterações de configuração para esses tipos de recursos especificados, independentemente de você definir o `includeGlobalResourceTypes` campo como false.
>
> Se você não quiser gravar as alterações na configuração dos tipos globais de recursos do IAM (usuários, grupos e perfis do IAM e políticas gerenciadas pelo cliente), não as liste no campo `resourceTypes`, além de definir o campo `includeGlobalResourceTypes` como falso.

O arquivo `recordingGroup.json` especifica que tipos de recursos o AWS Config registrará.

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

ii. O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--configuration-recorder`:

- `name`— O nome do gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração.
- `roleARN`— Amazon Resource Name (ARN) da função do IAM assumida AWS Config e usada pelo gravador de configuração.
- `recordingMode`— Especifica a frequência de gravação padrão AWS Config usada para registrar as alterações de configuração. AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.

- `recordingFrequency`— A frequência de gravação padrão AWS Config usada para registrar alterações na configuração.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- `recordingModeOverrides`: esse campo permite especificar as substituições para o modo de gravação. É uma matriz de objetos `recordingModeOverride`. Cada objeto `recordingModeOverride` na matriz `recordingModeOverrides` consiste em três campos:
  - `description`: uma descrição fornecida para a substituição.
  - `recordingFrequency`: a frequência de gravação que será aplicada a todos os tipos de recursos especificados na substituição.
  - `resourceTypes`— Uma lista separada por vírgulas que especifica quais tipos de recursos AWS Config estão incluídos na substituição.

> **Note**
>
> Campos obrigatórios e opcionais
> O campo `recordingMode` para `put-configuration-recorder` é opcional. Por padrão, a frequência de gravação do gravador de configuração é definida como gravação contínua.

> **Note**
>
> Limites
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Para a estratégia de gravação Registrar todos os tipos de recursos compatíveis atuais e futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), esses tipos de recursos serão definidos como Gravação contínua.

O `configurationRecorder.json` arquivo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Opcional) Para verificar se o seu gravador de configuração tem as configurações que você quer, use o comando a seguir `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

O seguinte é um exemplo de resposta.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
```

```
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

Configure AWS Config para registrar as alterações de configuração para todos os tipos de recursos compatíveis atuais e futuros, incluindo tipos de recursos globais, exceto os tipos de recursos que você especifica para excluir da gravação. Se você optar por interromper a gravação de um tipo de recurso, os itens de configuração que já foram gravados permanecerão inalterados. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

Esse comando usa `--configuration-recorder` os `---recording-group` campos e.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Grupo de gravação e gravador de configuração
>
> O campo `--recording-group` especifica quais tipos de recursos são gravados.

O `--configuration-recorder` campo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

1. Use o comando `put-configuration-recorder` e transfira um ou mais tipos de recursos a serem excluídos no campo `resourceTypes` de `exclusionByResourceTypes`, conforme mostrado no exemplo a seguir.

   i. O arquivo `recordingGroup.json` especifica que tipos de recursos o AWS Config registrará.

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

   Antes de especificar os tipos de recursos a serem excluídos na gravação:

   - Você deve definir os campos `allSupported` e `includeGlobalResourceTypes` do parâmetro `--recording-group` como `false`, ou omiti-los.
   - Você deve definir o campo `useOnly` de `RecordingStrategy` para `EXCLUSION_BY_RESOURCE_TYPES`.

   Note

   Campos de substituição

Se você escolher `EXCLUSION_BY_RESOURCE_TYPES` para a estratégia de gravação, o campo `exclusionByResourceTypes` substituirá outras propriedades na solicitação.
Por exemplo, mesmo que você defina `includeGlobalResourceTypes` como falso, os tipos de recursos globais do IAM ainda serão gravados automaticamente nessa opção, a menos que esses tipos de recursos estejam especificamente listados como exclusões no campo `resourceTypes` de `exclusionByResourceTypes`.

> **Note**
>
> Tipos de recursos globais e a estratégia de gravação de exclusão de recursos
> Por padrão, se você escolher a estratégia de `EXCLUSION_BY_RESOURCE_TYPES` gravação, quando AWS Config adiciona suporte para um novo tipo de recurso na região em que você configurou o gravador de configuração, incluindo tipos de recursos globais, AWS Config começa a gravar recursos desse tipo automaticamente.
> A menos que seja especificamente listado como exclusões, `AWS::RDS::GlobalCluster` será gravado automaticamente em todas as AWS Config regiões suportadas onde o gravador de configuração estiver ativado.
> Usuários, grupos, funções e políticas gerenciadas pelo cliente do IAM serão registrados na região em que você configurou o gravador de configuração, se essa for uma região em que AWS Config estava disponível antes de fevereiro de 2022.
> Você não pode registrar os tipos de recursos globais do IAM nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

ii. O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--configuration-recorder`:

- `name`— O nome do gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração.
- `roleARN`— Amazon Resource Name (ARN) da função do IAM assumida AWS Config e usada pelo gravador de configuração.
- `recordingMode`— Especifica a frequência de gravação padrão AWS Config usada para registrar as alterações na configuração. AWS Config suporta gravação contínua e

gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.

- `recordingFrequency`— A frequência de gravação padrão AWS Config usada para registrar alterações na configuração.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- `recordingModeOverrides`: esse campo permite especificar as substituições para o modo de gravação. É uma matriz de objetos `recordingModeOverride`. Cada objeto `recordingModeOverride` na matriz `recordingModeOverrides` consiste em três campos:
  - `description`: uma descrição fornecida para a substituição.
  - `recordingFrequency`: a frequência de gravação que será aplicada a todos os tipos de recursos especificados na substituição.
  - `resourceTypes`— Uma lista separada por vírgulas que especifica quais tipos de recursos AWS Config estão incluídos na substituição.

> **Note**
>
> Campos obrigatórios e opcionais
> O campo `recordingMode` para `put-configuration-recorder` é opcional. Por padrão, a frequência de gravação do gravador de configuração é definida como gravação contínua.

> **Note**
>
> Limites
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`

- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Para a estratégia de gravação Registrar todos os tipos de recursos compatíveis atuais e futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), esses tipos de recursos serão definidos como Gravação contínua.

O `configurationRecorder.json` arquivo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Opcional) Para verificar se o seu gravador de configuração tem as configurações que você quer, use o comando a seguir `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

O seguinte é um exemplo de resposta.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
```

```
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

Configure AWS Config para registrar as alterações de configuração somente para os tipos de recursos que você especificar. Se você optar por interromper a gravação de um tipo de recurso, os itens de configuração que já foram gravados permanecerão inalterados.

Esse comando usa `--configuration-recorder` os `---recording-group` campos e.

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

> **Note**
>
> Grupo de gravação e gravador de configuração
>
> O campo `--recording-group` especifica quais tipos de recursos são gravados. O `--configuration-recorder` campo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

1. Use o comando `put-configuration-recorder` e transfira um ou mais tipos de recursos no campo `resourceTypes` do `recordingGroup`, conforme mostrado no seguinte exemplo.
   i. O arquivo `recordingGroup.json` especifica que tipos de recursos o AWS Config registrará.

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": false,
    "resourceTypes": [
        "AWS::EC2::EIP",
        "AWS::EC2::Instance",
        "AWS::EC2::NetworkAcl",
        "AWS::EC2::SecurityGroup",
        "AWS::CloudTrail::Trail",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC",
        "AWS::IAM::User",
        "AWS::IAM::Policy"
  ]
}
```

> **Note**
>
> Campos obrigatórios e opcionais

Antes de especificar os tipos de recursos a serem incluídos na gravação, você deve definir os campos `allSupported` e `includeGlobalResourceTypes` como `false`, ou omiti-los.
O campo `recordingStrategy` é opcional quando você lista os tipos de recursos no campo `resourceTypes` de `--recording-group`.

> **Note**
>
> Disponibilidade de regiões
> Antes de especificar um tipo de recurso AWS Config para rastrear, verifique a disponibilidade da cobertura de recursos por região para ver se o tipo de recurso é suportado na AWS região em que você AWS Config configurou. Se um tipo de recurso for suportado AWS Config em pelo menos uma região, você poderá habilitar o registro desse tipo de recurso em todas as regiões suportadas pelo AWS Config, mesmo que o tipo de recurso especificado não seja suportado na AWS região em que você configurou AWS Config.

ii. O `put-configuration-recorder` usa os seguintes campos para o parâmetro `--configuration-recorder`:

- `name`— O nome do gravador de configuração. AWS Config atribui automaticamente o nome de “padrão” ao criar o gravador de configuração.
- `roleARN`— Amazon Resource Name (ARN) da função do IAM assumida AWS Config e usada pelo gravador de configuração.
- `recordingMode`— Especifica a frequência de gravação padrão AWS Config usada para registrar as alterações na configuração. AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.
  - `recordingFrequency`— A frequência de gravação padrão AWS Config usada para registrar alterações na configuração.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

- `recordingModeOverrides`: esse campo permite especificar as substituições para o modo de gravação. É uma matriz de objetos `recordingModeOverride`. Cada objeto `recordingModeOverride` na matriz `recordingModeOverrides` consiste em três campos:
  - `description`: uma descrição fornecida para a substituição.
  - `recordingFrequency`: a frequência de gravação que será aplicada a todos os tipos de recursos especificados na substituição.
  - `resourceTypes`— Uma lista separada por vírgulas que especifica quais tipos de recursos AWS Config estão incluídos na substituição.

> **Note**
>
> Campos obrigatórios e opcionais
>
> O campo `recordingMode` para `put-configuration-recorder` é opcional. Por padrão, a frequência de gravação do gravador de configuração é definida como gravação contínua.

> **Note**
>
> Limites
>
> A gravação diária não é compatível com os seguintes tipos de recursos:
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> Para a estratégia de gravação Registrar todos os tipos de recursos compatíveis atuais e futuros (`ALL_SUPPORTED_RESOURCE_TYPES`), esses tipos de recursos serão definidos como Gravação contínua.

O `configurationRecorder.json` arquivo especifica `name` e `roleArn` também a frequência de gravação padrão para o gravador de configuração ()`recordingMode`. Também é possível usar esse campo para substituir a frequência de gravação de tipos de recursos específicos.

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to
 include in the override ]
        }
    ]
  }
}
```

2. (Opcional) Para verificar se o seu gravador de configuração tem as configurações que você quer, use o comando a seguir `describe-configuration-recorders`.

```
$ aws configservice describe-configuration-recorders
```

O seguinte é um exemplo de resposta.

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
```

```
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Frequência de gravação

AWS Config suporta gravação contínua e gravação diária. A gravação contínua possibilita gravar as alterações na configuração de modo contínuo sempre que ocorre uma alteração. Gravação contínua: você vai receber um item de configuração (CI) que representa o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado.

Gravação contínua

São alguns benefícios da gravação contínua:

- Monitoramento em tempo real: a gravação contínua pode oferecer detecção imediata de alterações não autorizadas ou alterações inesperadas, o que pode aprimorar os esforços de segurança e conformidade.
- Análise detalhada: a gravação contínua pode permitir que você realize uma análise aprofundada das alterações de configuração nos recursos à medida que elas ocorrem, o que permite identificar padrões e tendências no momento.

Gravação diária

São alguns benefícios da gravação diária:

- Interrupção mínima: a gravação diária pode oferecer um fluxo de informações mais gerenciável, o que pode reduzir a frequência das notificações e a fadiga por alertas.
- Economia: a gravação diária pode oferecer a flexibilidade de gravar alterações nos recursos com uma frequência menor, o que pode reduzir os custos relacionados ao número de alterações de configuração gravadas.

> **Note**
>
> AWS Firewall Manager depende da gravação contínua para monitorar seus recursos. Se você estiver usando o Firewall Manager, é recomendável definir a frequência de gravação como Contínua.

Interromper a gravação de recursos

Você pode parar AWS Config de gravar um tipo de recurso a qualquer momento. Depois de AWS Config interromper a gravação de um recurso, ele retém as informações de configuração que foram capturadas anteriormente e você pode continuar acessando essas informações.

Recursos não gravados

Se um recurso não for registrado, AWS Config captura somente a criação e a exclusão desse recurso, e nenhum outro detalhe, sem nenhum custo para você. Quando um recurso não registrado é criado ou excluído, AWS Config envia uma notificação e exibe o evento na página de detalhes do recurso. A página de detalhes para um recurso não registrado fornece valores nulos para a maioria

dos detalhes de configuração, e não fornece informações sobre relacionamentos e alterações de configuração.

> **Note**
>
> Os tipos de recursos de `AWS::IAM::User`, `AWS::IAM::Policy`, `AWS::IAM::Group`, `AWS::IAM::Role` só capturarão os estados de criação (`ResourceNotRecorded`) e exclusão (`ResourceDeletedNotRecorded`), se o recurso for, ou tiver sido, selecionado anteriormente como um recurso a ser registrado no gravador de configuração.

> **Note**
>
> Os itens de configuração (CIs) para `ResourceNotRecorded` e `ResourceDeletedNotRecorded` não seguem o tempo de gravação típico para tipos de recursos. Esses tipos de recursos são registrados somente durante o processo periódico de definição de linha de base para o gravador de configuração, que ocorre em uma frequência menos frequente do que para os outros tipos de recursos.

As informações de relacionamento que AWS Config fornecem recursos registrados não são limitadas devido à falta de dados para recursos não registrados. Se um recurso registrado está relacionado a um recurso não registrado, esse relacionamento é fornecido na página de detalhes do recurso registrado.

AWS Config Regras e tipos de recursos globais

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos globais do IAM não podem ser registrados em regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Melhores práticas para relatar conformidade em recursos globais integrados antes de fevereiro de 2022

Para evitar avaliações desnecessárias, você só deve implantar AWS Config regras e pacotes de conformidade que tenham esses recursos globais no escopo de uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional. Isso se aplica a AWS Config regras, AWS Config regras organizacionais e também regras criadas por outros AWS serviços, como AWS Security Hub AWS Control Tower e.

Se você não estiver gravando os tipos de recursos globais integrados antes de fevereiro de 2022, é recomendável não habilitar as seguintes regras periódicas para evitar avaliações desnecessárias:

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

Melhores práticas para relatar conformidade em recursos globais integrados após fevereiro de 2022

Os tipos de recursos globais integrados à AWS Config gravação após fevereiro de 2022 serão registrados somente na região de origem do serviço para a partição comercial e AWS GovCloud (Oeste dos EUA) para a partição. AWS GovCloud (US) Você deve implantar AWS Config regras e pacotes de conformidade que tenham esses recursos globais no escopo somente na região de origem do tipo de recurso. Para obter mais informações, consulte Regiões de origem para tipos de recursos globais.

Configurações de registro para recursos de terceiros

Registre configurações para recursos de terceiros ou tipos de recursos personalizados, como servidores locais, ferramentas de monitoramento SAAS e sistemas de controle de versão (semelhantes). GitHub Você pode publicar os dados de configuração de recursos de terceiros, visualizar AWS Config e monitorar o inventário de recursos e o histórico de configuração usando o AWS Config console e as APIs. Agora, você pode usar AWS Config para gerenciar todos os seus recursos e avaliar a configuração dos recursos quanto à conformidade com as melhores práticas usando AWS Config regras. Você também pode criar AWS Config regras ou pacotes de conformidade para avaliar esses recursos de terceiros em relação às melhores práticas, políticas internas e políticas regulatórias.

> **Note**
>
> Se você tiver configurado AWS Config para registrar todos os tipos de recursos, os recursos de terceiros gerenciados (criados, atualizados ou excluídos) por meio deles AWS CloudFormation serão automaticamente rastreados AWS Config como itens de configuração.

Pré-requisito: os recursos de terceiros ou o tipo de recurso personalizado devem ser registrados usando. AWS CloudFormation

Tópicos

- Etapa 1: Configurar o ambiente de desenvolvimento
- Etapa 2: Modelar seu recurso
- Etapa 3: gerar artefatos
- Etapa 4: registrar o recurso
- Etapa 5: publicar a configuração do recurso
- Registre e exclua um estado de configuração para recursos de terceiros usando AWS CLI
- Gerenciar um estado de configuração para os tipos de recursos de terceiros usando APIs

Etapa 1: Configurar o ambiente de desenvolvimento

Instale e configure AWS CloudFormation AWS CLI. AWS CLI Isso permite que você modele e registre seus recursos personalizados. Para obter mais informações, consulte Recursos personalizados e O que é a interface de linha de CloudFormation comando? .

Etapa 2: Modelar seu recurso

Crie um esquema de provedor de recursos que esteja em conformidade com a configuração do tipo de recurso e faça sua validação.

1. Use o comando `init` para criar seu projeto de provedor de recursos e gerar os arquivos necessários.

```
$ cfn init
Initializing new project
```

2. O comando `init` inicia um assistente que orienta você na configuração do projeto, incluindo a especificação do nome do recurso. Para esta demonstração, especifique `MyCustomNamespace::Testing::WordPress`.

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. Insira um nome de pacote para o recurso.

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

> **Note**
>
> Para garantir que todas as dependências do projeto sejam resolvidas corretamente, você pode importar o projeto gerado para o seu IDE com o suporte do Maven. Por exemplo, se estiver usando o IntelliJ IDEA, você precisará fazer o seguinte:
>
> - No menu Arquivo, escolha Novo, em seguida, escolha Projeto das origens existentes.
> - Navegue até o diretório de projeto
> - Na caixa de diálogo Importar projeto, escolha Importar projeto do modelo externo e, em seguida, escolha Maven.
> - Escolha Avançar e aceite todos os padrões para concluir a importação do projeto.

4. Abra o arquivo `mycustomnamespace-testing-wordpress.json` que contém o esquema para o recurso. Copie e cole o esquema a seguir em `mycustomnamespace-testing-wordpress.json`.

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. Valide o esquema.

```
$ cfn validate
```

6. Atualize os arquivos gerados automaticamente no pacote do provedor de recursos para visualizar as atualizações do esquema do provedor de recursos. Após o início do projeto do

provedor de recursos, AWS CLI ele gera arquivos e códigos de suporte para o provedor de recursos. Gere novamente o código para ver o esquema atualizado.

```
$ cfn generate
```

> **Note**
>
> Ao usar o Maven, como parte do processo de criação, o comando `generate` é executado automaticamente antes que o código seja compilado. Portanto, suas alterações nunca sairão de sincronia com o código gerado.
> Esteja ciente de que a CloudFormation CLI deve estar em um local que o Maven/o sistema possa encontrar. Para obter mais informações, consulte Setting up your environment for developing extensions.

Para obter mais informações, consulte Modeling Resource Providers for Use in AWS CloudFormation.

Etapa 3: gerar artefatos

Execute o comando a seguir para gerar artefatos para o `cfn submit`.

```
$ mvn package
```

Etapa 4: registrar o recurso

AWS Config não exige que os manipuladores do provedor de recursos realizem o rastreamento da configuração do seu recurso. Execute o comando a seguir para registrar o recurso.

```
$ cfn submit
```

Para obter mais informações, consulte Registrando provedores de recursos para uso em AWS CloudFormation modelos.

Etapa 5: publicar a configuração do recurso

Determine a configuração para MyCustomNamespace: :Testing::WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

Determine a ID da versão do esquema a partir de AWS CloudFormation `DescribeType`.

No AWS Config veja se essa configuração de recurso é aceita. Para avaliar a conformidade, você pode AWS Config criar regras usando esse recurso. Para obter informações adicionais, consulte Registrar e excluir um estado de configuração para recursos de terceiros usando a AWS CLI.

Opcional: para automatizar a gravação da configuração, implemente coletores de configuração periódicos ou baseados em alterações.

Registre e exclua um estado de configuração para recursos de terceiros usando AWS CLI

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, insira `aws configure` para configurar o AWS CLI para usar uma AWS região em que AWS Config os agregadores estejam disponíveis.

Tópicos

- Registrar um item de configuração
- Leia o item de configuração usando as APIs do AWS Config
- Excluir o recurso de terceiros

Registrar um item de configuração

Registre um item de configuração para um recurso de terceiros ou um tipo de recurso personalizado usando o seguinte procedimento:

Certifique-se de registrar o tipo de recurso `MyCustomNamespace::Testing::WordPress` com seu esquema correspondente.

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando :

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> Conforme definido no esquema de tipos, `writeOnlyProperties` será removido da configuração antes de ser gravado pelo AWS Config. Isso significa que esses valores não estarão presentes quando a configuração for obtida por meio de APIs de leitura. Para obter mais informações, sobre `writeOnlyProperties`, consulte Resource type schema.

Leia o item de configuração usando as APIs do AWS Config

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando :

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. Pressione Enter.

   Você deve ver saída semelhante a:

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. Digite o comando :

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. Pressione Enter.

   Você deve ver saída semelhante a:

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

Excluir o recurso de terceiros

É possível registrar o estado de configuração para um recurso de terceiros ou tipo de recurso personalizado que você deseja excluir.

- Digite o comando :

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

  Se for bem sucedido, o comando será executado sem saída adicional.

Gerenciar um estado de configuração para os tipos de recursos de terceiros usando APIs

Você pode gerenciar um estado de configuração para recursos de terceiros ou tipo de recurso personalizado usando PutResourceConfig e Config DeleteResource APIs. Para obter mais informações, consulte a Referência da API do .

- PutResourceConfig
- DeleteResourceConfig

Registrar a configuração de software para instâncias gerenciadas

Você pode usar AWS Config para registrar alterações no inventário de software em instâncias do Amazon EC2 e servidores locais. Isso permite que você consulte as mudanças históricas na configuração de software. Por exemplo, quando uma nova atualização do Windows é instalada em uma instância gerenciada do Windows, AWS Config registra as alterações e as envia ao seu canal de entrega, para que você seja notificado sobre a alteração. Com AWS Config, você pode ver o histórico de quando as atualizações do Windows foram instaladas para a instância gerenciada e como elas mudaram ao longo do tempo.

Você deve executar as seguintes etapas para registrar as alterações de configuração de software:

- Ative o registro para o tipo de recurso do inventário de instância gerenciada no AWS Config.
- Configure o EC2 e servidores no local como instâncias gerenciadas no AWS Systems Manager. Uma instância gerenciada é uma máquina que foi configurada para uso com o Systems Manager.

- Inicie a coleta do inventário de software de suas instâncias gerenciadas usando o recurso de inventário do Systems Manager Inventory.

> **Note**
>
> O Systems Manager agora oferece suporte à criação de itens de configuração para instâncias não gerenciadas
> O item de configuração para instâncias não gerenciadas terá configuração suplementar com `Key: “InstanceStatus”` e `Value: “Unmanaged”`.
> Os itens de configuração para instâncias não gerenciadas não receberão atualizações adicionais
> Para receber atualizações adicionais, o item de configuração deve ser uma instância gerenciada.

Você também pode usar AWS Config regras para monitorar alterações na configuração do software e ser notificado se as alterações estão em conformidade ou não com suas regras. Por exemplo, se você criar uma regra que verifique se suas instâncias gerenciadas têm um aplicativo especificado e se uma instância não tem esse aplicativo instalado, AWS Config sinalize essa instância como não compatível com sua regra. Para obter uma lista de regras AWS Config gerenciadas, consulteLista de regras AWS Config gerenciadas.

Para ativar o registro de alterações de configuração de software no AWS Config:

1. Ative o registro para todos os tipos de recursos com suporte ou, seletivamente, registre o tipo de recurso no inventário de instância gerenciada no AWS Config. Para ter mais informações, consulte AWS Recursos de gravação.
2. Inicie uma instância do Amazon EC2 com um perfil de instância para Systems Manager que inclua a política gerenciada do AmazonSSM ManagedInstanceCore. Essa política gerenciada da AWS permite que uma instância use a funcionalidade básica do serviço Systems Manager.

   Para obter informações sobre outras políticas que você pode adicionar ao perfil de instância do Systems Manager, consulte Create an IAM Instance Profile for Systems Manager no Guia do usuário do AWS Systems Manager .

> **Important**
>
> O SSM Agent é um software da Amazon que deve ser instalado em uma instância gerenciada para se comunicar com o Systems Manager na nuvem. Se a sua instância do EC2 foi criada a partir de uma AMI para um dos seguintes sistemas operacionais, o agente está pré-instalado:
>
> - AMIs do Windows Server 2003-2012 R2 publicadas em novembro de 2016 ou posteriormente
> - Windows Server 2016 e 2019
> - Amazon Linux
> - Amazon Linux 2
> - Ubuntu Server 16.04
> - Ubuntu Server 18.04
>
> Em instâncias do EC2 que não foram criadas a partir de uma AMI com o agente pré-instalado, você deve instalar o agente manualmente. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS Systems Manager :
>
> - Instalar e configurar o SSM Agent em instâncias EC2 do Windows
> - Instalar e configurar o SSM Agent em instâncias EC2 do Linux

3. Inicie a coleta de inventário, conforme descrito em Configurar a coleta de inventário no Guia do usuário do AWS Systems Manager . Os procedimentos são os mesmos para as instâncias Linux e Windows.

   AWS Config pode registrar alterações de configuração para os seguintes tipos de inventário:

   - Aplicações: uma lista dos aplicações para instâncias gerenciadas, como software antivírus.
   - AWS componentes — Uma lista de AWS componentes para instâncias gerenciadas, como AWS CLI e SDKs.
   - Informações sobre a instância: informações sobre a instância, como nome e versão do SO, domínio e status do firewall.
   - Configuração de rede: informações de configuração, como endereço IP, gateway e máscara de sub-rede.

- Atualizações do Windows: uma lista de atualizações do Windows para instâncias gerenciadas (somente instâncias Windows).

> **Note**
>
> AWS Config não suporta o registro do tipo de inventário personalizado no momento.

A coleta de inventário é um dos muitos recursos do Systems Manager que são agrupados nas categorias Gerenciamento de operações, Ações e alterações, Instâncias e nós e Recursos compartilhados. Para obter mais informações, consulte O que é o Systems Manager? e Recursos do Systems Manager no Guia do usuário do AWS Systems Manager .

Exibir histórico e configurações de recursos da

Você pode visualizar todos os recursos que estão AWS Config sendo registrados em sua conta, as alterações de configuração que ocorreram em um recurso durante um período de tempo especificado e as relações do recurso selecionado com todos os recursos relacionados. Você também pode visualizar as alterações do estado de conformidade dos recursos, conforme avaliadas, Regras do AWS Config exibidas em um cronograma.

Tópicos

- Pesquisando recursos que são descobertos por AWS Config
- Visualizando informações de conformidade e resultados da avaliação
- Visualizando o histórico de configuração e conformidade

Pesquisando recursos que são descobertos por AWS Config

Você pode usar o AWS Config console e a AWS Config API para pesquisar os recursos que foram inventariados AWS Config ou descobertos, incluindo recursos excluídos e recursos que AWS Config não estão sendo gravados no momento. AWS CLI AWS Config descobre somente os tipos de recursos compatíveis. Para ter mais informações, consulte Tipos de recursos compatíveis.

Pesquisa por recursos (Console)

Você pode usar tipos de recursos ou informações de tag para pesquisar recursos no console AWS Config .

Para pesquisar recursos (Console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Na página Resource inventory, especifique as opções de pesquisa para os recursos que você deseja pesquisar:
   - Categoria de recursos — Escolha todas as categorias de recursos ou restrinja os resultados somente a AWS Recursos.
   - Tipo de recurso: escolha todos os tipos de recursos ou selecione por quais recursos filtrar.
   - Conformidade: opte por filtrar por qualquer status de conformidade, compatível ou não compatível.
3. AWS Config lista os recursos que correspondem às suas opções de pesquisa. Você pode ver as seguintes informações sobre os recursos:
   - Identificador de recursos: o identificador de recursos pode ser um ID ou um nome de recurso, se aplicável. Escolha o link de identificador de recursos para exibir a página de detalhes do recurso.
   - Tipo de recurso: o tipo de recurso é listado.
   - Conformidade — O status do recurso AWS Config avaliado de acordo com sua regra.

     Para ter mais informações, consulte Visualizando o histórico de configuração e conformidade.

Pesquisar recursos (AWS CLI)

Você pode usar o AWS CLI para listar os recursos que AWS Config foram descobertos.

Para examinar recursos (AWS CLI)

Use o comando AWS Config service **`list-discovered-resources`**:

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
```

```
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
        }
```

Para visualizar os detalhes da configuração de um recurso que está listado na resposta, use o comando `get-resource-config-history` e especifique o tipo de recurso e ID. Para obter um exemplo desse comando e da resposta de AWS Config, consulteVisualizar o histórico de configuração.

Pesquisar por recursos (API)

Você especifica um tipo de recurso e AWS Config retorna uma lista de identificadores de recursos para recursos desse tipo. Para obter mais informações, consulte ResourceIdentifiera Referência AWS Config da API.

Para pesquisar recursos (API)

Use a ação ListDiscoveredResources.

Para obter os detalhes de configuração de um recurso listado na resposta, use a GetResourceConfigHistoryação e especifique o tipo e a ID do recurso.

Visualizando informações de conformidade e resultados da avaliação

> **Important**
>
> Para obter relatórios precisos sobre o status de conformidade, você deve registrar o tipo de recurso do `AWS::Config::ResourceCompliance`. Para obter mais informações, consulte AWS Recursos de recodificação.

Você pode usar o AWS Config console ou AWS os SDKs para visualizar as informações de conformidade e os resultados da avaliação de suas regras e recursos.

Sumário

- Exibir a conformidade (console)
- Visualizando a conformidade (AWS SDKs)

Exibir a conformidade (console)

Para ver a conformidade (Console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. No painel de navegação, escolha Resources (Recursos). Na página Inventário de recursos, você pode filtrar por categoria de recurso, tipo de recurso e status de conformidade. Escolha Incluir recursos excluídos, se apropriado. A tabela exibe o identificador do tipo de recurso e o status de compatibilidade desse recurso. O identificador de recursos pode ser um ID ou um nome de recurso.
4. Selecione o recurso na coluna de identificador de recurso.
5. Escolha o botão Cronograma do recurso. Você pode filtrar por eventos de configuração, eventos de conformidade ou CloudTrail eventos.

> **Note**
>
> Como alternativa, na página Inventário de recursos, você pode clicar no nome do recurso. Para acessar o cronograma de recursos na página de detalhes do recurso, escolha o botão Cronograma do recurso.

Você também pode exibir a compatibilidade de seus recursos procurando-os na página Resource inventory (Inventário de recursos). Para ter mais informações, consulte Pesquisando recursos que são descobertos por AWS Config.

Visualizando a conformidade (AWS SDKs)

Para obter informações de conformidade para suas AWS Config regras

Os exemplos de códigos a seguir mostram como usar `DescribeComplianceByConfigRule`.

CLI

AWS CLI

Para obter informações de conformidade para suas regras de AWS Config

O comando a seguir retorna informações de conformidade para cada regra AWS do Config que é violada por um ou mais recursos: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos não estão em conformidade com a regra relacionada. Por exemplo, a saída a seguir indica que três recursos não estão em conformidade com a regra nomeada`InstanceTypesAreT2micro`.

Saída:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeComplianceByConfigRuleem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo recupera detalhes de conformidade da regra ebs-optimized-instance, para os quais não há resultados de avaliação atuais para a regra, portanto, retorna INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Saída:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Exemplo 2: Esse exemplo retorna o número de recursos não compatíveis para a regra ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Saída:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obter detalhes da API, consulte DescribeComplianceByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter informações de conformidade para seus AWS recursos

Os exemplos de códigos a seguir mostram como usar `DescribeComplianceByResource`.

CLI

AWS CLI

Para obter informações de conformidade para seus AWS recursos

O comando a seguir retorna informações de conformidade para cada instância do EC2 que é registrada pelo AWS Config e que viola uma ou mais regras:

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Na saída, o valor de cada `CappedCount` atributo indica quantas regras o recurso viola. Por exemplo, a saída a seguir indica que a instância `i-1a2b3c4d` viola duas regras.

Saída:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeComplianceByResourceem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo verifica o tipo **`AWS::SSM::ManagedInstanceInventory`** de recurso quanto ao tipo de conformidade “COMPATÍVEL”.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Saída:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obter detalhes da API, consulte DescribeComplianceByResourceem Referência de AWS Tools for PowerShell cmdlet.

Para obter o resumo de conformidade de suas AWS Config regras

Os exemplos de códigos a seguir mostram como usar `GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Para obter o resumo de conformidade de suas regras de AWS Config

O comando a seguir retorna o número de regras que estão em conformidade e o número que não estão em conformidade:

```
aws configservice get-compliance-summary-by-config-rule
```

Na saída, o valor de cada `CappedCount` atributo indica quantas regras estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByConfigRuleem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna o número de regras do Config que não estão em conformidade.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Saída:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obter detalhes da API, consulte GetComplianceSummaryByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter o resumo de conformidade de seus AWS recursos

Os exemplos de códigos a seguir mostram como usar `GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Para obter o resumo de conformidade de todos os tipos de recursos

O comando a seguir retorna o número de AWS recursos que não estão em conformidade e o número que estão em conformidade:

```
aws configservice get-compliance-summary-by-resource-type
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Para obter o resumo de conformidade de um tipo específico de recurso

O comando a seguir retorna o número de instâncias do EC2 que não estão em conformidade e o número que estão em conformidade:

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByResourceTypeem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna o número de recursos compatíveis ou não compatíveis e converte a saída em json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
```

```
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByResourceTypeem Referência de AWS Tools for PowerShell cmdlet.

Para obter os resultados da avaliação de uma AWS Config regra

Os exemplos de códigos a seguir mostram como usar `GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Para obter os resultados da avaliação de uma regra AWS Config

O comando a seguir retorna os resultados da avaliação de todos os recursos que não estão em conformidade com uma regra de AWS Config chamada: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Saída:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
```

```
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceDetailsByConfigRuleem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo obtém os resultados da avaliação da regra access-keys-rotated e retorna a saída agrupada por tipo de conformidade

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Saída:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Exemplo 2: Este exemplo consulta os detalhes de conformidade da regra access-keys-rotated para recursos COMPATÍVEIS.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Saída:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obter detalhes da API, consulte GetComplianceDetailsByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter os resultados da avaliação de um AWS recurso

Os exemplos de códigos a seguir mostram como usar `GetComplianceDetailsByResource`.

CLI

AWS CLI

Para obter os resultados da avaliação de um AWS recurso

O comando a seguir retorna os resultados da avaliação de cada regra com a qual a instância do EC2 `i-1a2b3c4d` não está em conformidade:

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Saída:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceDetailsByResourceem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo de resultados de avaliação para o recurso fornecido.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Saída:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obter detalhes da API, consulte GetComplianceDetailsByResourceem Referência de AWS Tools for PowerShell cmdlet.

Visualizando o histórico de configuração e conformidade

> **Important**
>
> Para obter relatórios precisos sobre o status de conformidade, você deve registrar o tipo de recurso do `AWS::Config::ResourceCompliance`. Para obter mais informações, consulte AWS Recursos de recodificação.

Você pode visualizar a configuração, os relacionamentos e o número de alterações feitas em um recurso no AWS Config console. Você pode visualizar o histórico de configuração de um recurso usando AWS CLI.

Exibir detalhes de configuração (console)

Exibindo detalhes da configuração usando o console

Quando você pesquisar recursos na página Inventário de recursos, clique no nome ou no ID do recurso na coluna de identificadores de recursos para exibir a página de detalhes do recurso. A página de detalhes fornece informações sobre a configuração, relacionamentos e o número de alterações feitas para aquele recurso.

Para acessar o cronograma de recursos na página de detalhes do recurso, escolha o botão Cronograma do recurso. O cronograma de recursos captura alterações como `ConfigurationItems` durante um período para um recurso específico. Você pode filtrar por eventos de configuração, eventos de conformidade ou CloudTrail eventos.

Visualizar detalhes da configuração (AWS CLI)

Exibindo detalhes da configuração usando o AWS CLI

Os itens de configuração que AWS Config registra são entregues ao canal de entrega especificado sob demanda como um instantâneo da configuração e como um fluxo de configuração. Você pode usar o AWS CLI para visualizar o histórico dos itens de configuração de cada recurso.

Visualizar o histórico de configuração

Digite o comando `get-resource-config-history` e especifique o tipo de recurso e o ID do recurso; por exemplo:

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
```

```
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

Para uma explicação detalhada dos campos de resposta, consulte Components of a Configuration Item e Tipos de recursos compatíveis.

Exemplo de histórico de configuração do Amazon EBS do AWS Config

AWS Config gera um conjunto de arquivos, cada um representando um tipo de recurso e lista todas as alterações de configuração dos recursos desse tipo que AWS Config está gravando. AWS Config exporta esse histórico de configuração centrado em recursos como um objeto no bucket do Amazon S3 que você especificou quando habilitou. AWS Config O arquivo de histórico de configuração para cada tipo de recurso contém as alterações que foram detectadas para os recursos daquele tipo desde que o último arquivo de histórico foi entregue. Os arquivos de histórico normalmente são entregues a cada seis horas.

A seguir está um exemplo do conteúdo do objeto Amazon S3 que descreve o histórico de configuração de todos os volumes do Amazon Elastic Block Store na região atual para você. Conta da AWS Os volumes nessa conta incluem `vol-ce676ccc` e `vol-cia007c`. O volume `vol-ce676ccc` tinha duas alterações de configuração desde a entrega do arquivo de histórico anterior, enquanto o `vol-cia007c` tinha uma alteração.

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
```

```
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-ce676ccc",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-ad229edbb1e4",
```

```
                "c376e30d-71a2-4694-89b7-a5a04w292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
```

```
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
```

```
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

Visualizar o cronograma do histórico de conformidade para recursos

AWS Config suporta o armazenamento de alterações do estado de conformidade dos recursos, conforme avaliado por Regras do AWS Config. O histórico de compatibilidade de recursos é apresentado na forma de um cronograma. O cronograma captura alterações como `ConfigurationItems` ao longo de um período para um recurso específico. Para obter informações sobre o conteúdo de`ConfigurationItem`, consulte ConfigurationItemna Referência AWS Config da API.

Você pode aceitar ou cancelar o registro de todos os tipos de recurso no AWS Config. Se você optou por registrar todos os tipos de recursos, começará AWS Config automaticamente a registrar o histórico de conformidade do recurso conforme avaliado por Regras do AWS Config. Por padrão, AWS Config registra as alterações de configuração de todos os recursos suportados. Você também pode selecionar apenas o tipo de recurso específico do histórico de conformidade de recursos: `AWS::Config::ResourceCompliance`. Para obter mais informações, consulte Selecionar quais AWS Config registros de recursos.

Visualizar o cronograma de recursos usando recursos

Acesse o cronograma de recursos selecionando um recurso específico na página Inventário de recursos.

1. Selecione os recursos na navegação à esquerda.
2. Na página Inventário de recursos, você pode filtrar por categoria de recurso, tipo de recurso e status de conformidade. Escolha Incluir recursos excluídos, se apropriado.

   A tabela exibe o identificador do tipo de recurso e o status de compatibilidade desse recurso. O identificador de recursos pode ser um ID ou um nome de recurso.
3. Selecione o recurso na coluna de identificador de recurso.

4. Escolha o botão Cronograma do recurso. Você pode filtrar por eventos de configuração, eventos de conformidade ou CloudTrail eventos.

> **Note**
>
> Como alternativa, na página Inventário de recursos, você pode clicar no nome do recurso. Para acessar o cronograma de recursos na página de detalhes do recurso, escolha o botão Cronograma do recurso.

Exibir o cronograma de recursos usando regras

Acesse o cronograma de recursos selecionando uma regra específica da página Regra.

1. Selecione as regras na navegação à esquerda.
2. Na página Regra, escolha uma regra que avalia seus recursos relevantes. Se nenhuma regra for exibida na tela, adicione regras com o botão Add rule (Adicionar regra).
3. Na página Rule details (Detalhes da regra), selecione os recursos na tabela Resources evaluated (Recursos avaliados).
4. Selecione o botão Cronograma do recurso. O cronograma do recurso é exibido.

Consultar histórico de conformidade

Consulte o histórico de conformidade do recurso get-resource-config-history usando o tipo de recurso`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

Você deve ver saída semelhante a:

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
```

```
      "resourceId": "configrules-bucket",
      "relationshipName": "Is associated with "
     }
    ]
    "tags": {},
    "resourceType": "AWS::Config::ResourceCompliance",
    "resourceId": "AWS::S3::Bucket/configrules-bucket",
    "ConfigurationStateId": "1539799966921",
    "relatedEvents": [];
    "awsRegion": "us-west-2",
    "version": "1.3",
    "configurationItemMD5Hash": "",
    "supplementaryConfiguration": {},
    "configuration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":
\"configrules-bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList"\":
[{\"configRuleArn\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw
\",\"configRuleId\":\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-
enabled\",\"complianceType\":\"COMPLIANT\"}]}",

    "configurationItemStatus": "ResourceDiscovered",
    "accountId": "AccountID"
   }
  ]
}
```

Marcar os recursos do AWS Config

Uma etiqueta é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você. As tags facilitam o gerenciamento, a pesquisa e a filtragem de recursos.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando há muitos recursos do mesmo tipo; você pode identificar rapidamente um recurso específico com base nas tags atribuídas a ele. Você pode atribuir uma ou mais tags aos seusAWS recursos. Cada tag tem um valor associado.

Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seusAWS recursos. É possível pesquisar e filtrar os recursos de acordo com as tags que adicionar.

As tags são interpretadas estritamente como uma string de caracteres e não são automaticamente atribuídas a seus recursos. É possível editar chaves de tags e valores, e é possível remover as tags de um recurso a qualquer momento. É possível definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

Você pode trabalhar com tags usando a AWS Command Line Interface (AWS CLI) e a referência de API do AWS Config.

Restrições relacionadas à marcação

As restrições básicas a seguir se aplicam às tags.

Restrição	Descrição
Número máximo de tags por recurso	50
Tamanho máximo da chave	128 caracteres do Unicode em UTF-8
Tamanho máximo do valor	256 caracteres Unicode em UTF-8
Restrição de prefixo	Não use o prefixo `aws:` no nome nem no valor de suas tags, pois ele é reservado para uso da AWS. Você não pode editar nem excluir nomes ou valores de tag com esse prefixo. As tags com esse prefixo não contam para as tags por limite de recurso.
Restrições de caracteres	As tags só podem conter letras Unicode, números, espaços em branco ou estes símbolos: `_ . : / = + - @`.

Gerenciar tags com ações de API do AWS Config

Controles de acesso com base em tags estão disponíveis para três recursos `ConfigurationAggregator`, `AggregationAuthorization` e `ConfigRule`. Use o seguinte para adicionar, atualizar, listar e excluir as tags para seus recursos.

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResourceeUntagResource` exigem certas permissõesAWS Identity and Access Management (IAM) para controlar o acesso. Para obter mais informações, consulte Controlar o acesso com base em chaves de tags no Guia do usuário do IAM.

Avaliação de recursos com regras AWS Config

Use AWS Config para avaliar as configurações dos seus AWS recursos. Você faz isso criando AWS Config regras, que representam suas configurações ideais. AWS Config fornece regras personalizáveis e predefinidas, chamadas de regras gerenciadas, para ajudar você a começar.

Como AWS Config as regras funcionam

Enquanto o AWS Config monitora continuamente as alterações de configuração que ocorrem entre seus recursos, ele verifica se essas alterações violam alguma das condições em suas regras. Se um recurso não estiver em conformidade com a regra, AWS Config sinaliza o recurso e a regra como não compatíveis. A seguir estão os possíveis resultados da avaliação de uma AWS Config regra:

- `COMPLIANT`: a regra passa pelas condições da verificação de conformidade.
- `NON_COMPLIANT`: a regra não cumpre as condições da verificação de conformidade.
- `ERROR`: um dos parâmetros obrigatórios/opcionais não é válido, não é do tipo correto ou está formatado incorretamente.
- `NOT_APPLICABLE`: usado para filtrar recursos aos quais a lógica da regra não pode ser aplicada. Por exemplo, a regra alb-desync-mode-check verifica somente os Application Load Balancers e ignora os Network Load Balancers e os Gateway Load Balancers.

Por exemplo, quando um volume EC2 é criado, AWS Config pode avaliar o volume em relação a uma regra que exige que os volumes sejam criptografados. Se o volume não estiver criptografado, AWS Config sinaliza o volume e a regra como não compatíveis. AWS Config também pode verificar todos os seus recursos para atender aos requisitos de toda a conta. Por exemplo, AWS Config pode verificar se o número de volumes do EC2 em uma conta permanece dentro do total desejado ou se uma conta usa AWS CloudTrail para registro.

Regras vinculadas a serviços

As regras vinculadas a serviços são um tipo exclusivo de regra gerenciada que permite que outros AWS serviços criem AWS Config regras em sua conta. Essas regras são predefinidas para incluir todas as permissões necessárias para ligar para outros AWS serviços em seu nome. Essas regras são semelhantes aos padrões que um AWS serviço recomenda em você Conta da AWS para verificação de conformidade. Para ter mais informações, consulte Regras vinculadas ao serviço AWS Config.

Regras personalizadas

Você também pode criar regras personalizadas para avaliar recursos adicionais que ainda AWS Config não foram registrados. Para obter mais informações, consulte AWS Config Regras personalizadas e Avaliar tipos de recursos adicionais.

Visualizando a conformidade

O AWS Config console mostra o status de conformidade de suas regras e recursos. Você pode ver como seus AWS recursos estão em conformidade geral com as configurações desejadas e saber quais recursos específicos não estão em conformidade. Você também pode usar a AWS CLI, a AWS Config API e os AWS SDKs para fazer solicitações ao AWS Config serviço para obter informações de conformidade.

Ao usar AWS Config para avaliar suas configurações de recursos, você pode avaliar se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes do setor e os regulamentos.

Limitações

Para ver o número máximo de AWS Config regras para cada região para cada conta e outros limites de serviço, consulte Limites AWS Config de serviço.

Considerações sobre custos

Para obter detalhes sobre os custos associados ao registro de recursos, consulte AWS Config preços.

Recomendação: pare de registrar a conformidade dos recursos antes de excluir as regras

É altamente recomendável que você interrompa a gravação do tipo de `AWS::Config::ResourceCompliance` recurso antes de excluir as regras da sua conta. A exclusão de regras cria itens de configuração (CIs) `AWS::Config::ResourceCompliance` e pode afetar os custos do gravador AWS Config de configuração. Se você estiver excluindo regras que avaliam um grande número de tipos de recursos, isso pode levar a um aumento no número de ICs registrados.

Melhor prática:

1. Pare de gravar `AWS::Config::ResourceCompliance`
2. Excluir regra (s)
3. Ativar a gravação para `AWS::Config::ResourceCompliance`

Recomendação: adicione lógica para lidar com a avaliação de recursos excluídos para regras lambda personalizadas

Ao criar regras lambda AWS Config personalizadas, é altamente recomendável que você adicione lógica para lidar com a avaliação dos recursos excluídos.

Quando os resultados da avaliação forem marcados como `NOT_APPLICABLE`, eles serão marcados para exclusão e limpos. Se NÃO estiverem marcados como`NOT_APPLICABLE`, os resultados da avaliação permanecerão inalterados até que a regra seja excluída, o que pode causar um aumento inesperado na criação de ICs `AWS::Config::ResourceCompliance` após a exclusão da regra.

Para obter informações sobre como definir regras lambda AWS Config personalizadas para retornar `NOT_APPLICABLE` para recursos excluídos, consulte Gerenciamento de recursos excluídos com regras lambda AWS Config personalizadas.

Recomendação: forneça os recursos no escopo das regras lambda personalizadas

AWS Config As regras personalizadas do Lambda podem causar um grande número de invocações de funções do Lambda se a regra não tiver como escopo um ou mais tipos de recursos. Para evitar o aumento da atividade associada à sua conta, é altamente recomendável fornecer recursos no escopo de suas regras personalizadas do Lambda. Se nenhum tipo de recurso for selecionado, a regra invocará a função do Lambda para todos os recursos na conta.

Suporte regional

Atualmente, o recurso de AWS Config regra é suportado nas seguintes AWS regiões. Para obter uma lista de quais AWS Config regras individuais são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
		config-fips.us-east-2.amazonaws.com	HTTPS
Leste dos EUA	us-east-1	config.us-east-1.amazonaws.com	HTTPS
		config-fips.us-east-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
(Norte da Virgínia)			
Oeste dos EUA (N. da Califórnia)	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
África (Cidade do Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milão)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Espanha)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurique)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

A implantação de AWS Config regras em contas de membros em uma AWS organização é suportada nas seguintes regiões.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (N. da	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Califórnia)			
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Componentes de uma AWS Config regra

AWS Config as regras avaliam as configurações dos seus AWS recursos. Há dois tipos de regras: regras gerenciadas pelo AWS Config e regras personalizadas do AWS Config .

AWS Config As regras gerenciadas são regras predefinidas e personalizáveis criadas por. AWS Config Para obter uma lista de regras gerenciadas, consulte Lista de regras AWS Config gerenciadas.

AWS Config Regras personalizadas são regras que você cria do zero. Há duas maneiras de criar regras AWS Config personalizadas: com as funções Lambda (Guia do AWS Lambda desenvolvedor) e com o Guard (Guard GitHub Repository), uma linguagem. policy-as-code AWS Config as regras personalizadas criadas com AWS Lambda são chamadas de Regras Lambda AWS Config Personalizadas e as regras AWS Config personalizadas criadas com o Guard são chamadas de Regras de Política AWS Config Personalizadas.

Esta página discute os metadados das regras AWS Config gerenciadas e as melhores práticas sobre como AWS Config criar regras personalizadas com Python usando o Rules Development Kit (RDK) e AWS Config a AWS Config Rules Development Kit Library (RDKlib).

Para ver um passo a passo mostrando como criar regras de política AWS Config personalizadas, consulte Criação de regras de política AWS Config personalizadas. Para ver um passo a passo mostrando como criar regras personalizadas do AWS Config Lambda, consulte Criação de regras personalizadas AWS Config do Lambda.

Sumário

- AWS Config metadados de regras gerenciadas
- AWS Config estrutura de regras personalizadas
  - Regras de escrita
  - Lógica da regra

AWS Config metadados de regras gerenciadas

AWS Config as regras gerenciadas podem conter os seguintes metadados mutáveis:

defaultName

O defaultName é o nome que as instâncias de uma regra receberão por padrão.

descrição

A description da regra fornece contexto sobre o que a regra avalia. O console do AWS Config tem um limite de 256 caracteres. Como prática recomendada, a descrição da regra deve começar com “Verifica se” e incluir uma descrição do cenário NON_COMPLIANT. Os nomes dos serviços devem ser escritos por extenso começando com AWS ou Amazon quando mencionados pela primeira vez na descrição da regra. Por exemplo, AWS CloudTrail ou Amazon CloudWatch em vez de CloudTrail ou CloudWatch para o primeiro uso. Os nomes dos serviços podem ser abreviados após referência subsequente.

scope

O escopo determina quais tipos de recursos a regra visa. Para obter uma lista de tipos de recursos compatíveis, consulte Supported Resource Types.

Detalhes obrigatórios InputParameter

Os compulsoryInputParameter detalhes são usados para parâmetros necessários para que uma regra faça sua avaliação. Por exemplo, a regra gerenciada do `access-keys-rotated` inclui `maxAccessKeyAge` como parâmetro obrigatório. Se um parâmetro for necessário, ele não será marcado como (Opcional). Para cada parâmetro, um tipo deve ser especificado. O tipo pode ser “String”, “int”, “double”, “CSV”, “boolean” e "StringMap”.

InputParameterDetalhes opcionais

Os optionalInputParameter Detalhes são usados para parâmetros que são opcionais para que uma regra faça sua avaliação. Por exemplo, a regra gerenciada `elasticsearch-logs-to-cloudwatch` inclui `logTypes` como parâmetro opcional. Para cada parâmetro, um tipo deve ser especificado. O tipo pode ser “String”, “int”, “double”, “CSV”, “boolean” e "StringMap”.

suportado EvaluationModes

supportedEvaluationModes Determina quando os recursos serão avaliados, antes de um recurso ser implantado ou depois de um recurso ter sido implantado.

`DETECTIVE` é usado para avaliar recursos que já foram implantados. Isso permite que você avalie as definições de configuração dos seus recursos existentes. `PROACTIVE` é usado para avaliar os recursos antes que eles sejam implantados.

Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

Você pode especificar o supportedEvaluationModes para `DETECTIVEPROACTIVE`,, ou ambos `DETECTIVE PROACTIVE` e. Você deve especificar um modo de avaliação e esse campo não pode permanecer vazio.

Para obter mais informações, consulte Modos de avaliação. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

AWS Config estrutura de regras personalizadas

Esta seção contém informações sobre como usar o AWS Config Rules Development Kit (RDK) e a AWS Config Rules Development Kit Library (RDKLib). Para obter mais informações sobre o RDK ou o RDKlib, consulte os repositórios e aws-config-rdklib. aws-config-rdk GitHub

Regras de escrita

Pré-requisitos

1. Siga as etapas em Instalação da AWS CLI.
2. Siga as etapas em Configurando AWS Config com o console ou Configurando AWS Config com AWS CLI o. Para obter informações sobre as AWS regiões em AWS Config que há suporte, selecione sua região na lista de serviços AWS regionais.
3. Instale o RDK usando o método recomendado com pip:

```
pip install rdk
```

> **Note**
>
> Antes de usar o pip, verifique se ele está instalado na sua máquina.

4. Instale a RDKLib usando o método recomendado com pip:

```
pip install rdklib
```

> **Note**
>
> Antes de usar o pip, verifique se ele está instalado na sua máquina.

Regras acionadas por mudanças

1. Para criar uma regra que seja acionada por uma mudança no tipo de recurso especificado, execute o seguinte comando:

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type
```

O exemplo a seguir cria uma regra que é acionada por uma mudança no tipo de recurso `AWS::IAM::User`:

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
```

A seguir estão os sinalizadores que você pode usar com o comando `rdk create` para regras acionadas por mudanças:

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

> **Note**
>
> Para usar a RDKlib, o tempo de execução da regra deve ser definido como `python3.6-lib`.

Depois de executar o `rdk create`, você deve ver um novo diretório com o nome da regra e três arquivos nele:

- *RULE_NAME*`.py`: arquivo Python onde a lógica da regra é armazenada.
- *RULE_NAME*`_test.py`: arquivo Python onde os testes unitários da regra são armazenados.
- `parameters.json`: arquivo JSON para as configurações de implantação do RDK.

2. A próxima etapa é escrever a lógica da regra. Você só precisará editar o arquivo *RULE_NAME*.py. Se você abrir o arquivo *RULE_NAME*.py, verá um modelo onde poderá adicionar a lógica das regras. Veja abaixo o modelo que foi gerado para MFA_ENABLED_RULE:

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

O exemplo a seguir é uma versão editada do modelo MFA_ENABLED_RULE com a lógica da regra. A regra verifica se os usuários do IAM têm autenticação multifator (MFA) habilitada. A regra será NON_COMPLIANT se um usuário do IAM não tiver a MFA habilitada. Para obter mais informações sobre a lógica de regras e os métodos fornecidos no modelo, consulte Lógica da regra.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

        # Scenario:1 IAM user has MFA enabled.
        if response["MFADevices"]:
            return [Evaluation(ComplianceType.COMPLIANT)]

        # Scenario:2 IAM user has MFA not enabled.
        annotation = "MFA needs to be enabled for user."
        return [Evaluation(ComplianceType.NON_COMPLIANT, annotation=annotation)]

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. A próxima etapa é instalar a camada RDKlib AWS com o AWS console ou. AWS CLI A RDKlib foi projetada para funcionar como uma camada do AWS Lambda . Ela permite que você use a biblioteca sem precisar incluí-la no pacote de implantação.

   - Para instalar a camada RDKlib com o AWS console, siga as seguintes etapas:

     1. Abra o AWS Serverless Application Repository console em https://console.aws.amazon.com/serverlessrepo.
     2. No menu de navegação à esquerda, escolha Aplicativos disponíveis.
     3. Pesquise `rdklib` e escolha rdklib.
     4. Revise os detalhes da função e implante-a. Nenhuma alteração deve ser necessária.
     5. Na seção Recursos na página Visão geral, copie o Amazon Resource Name (ARN) da camada Lambda. Você precisará do ARN da camada do Lambda ao implantar a regra.

   - Para instalar a camada RDKlib com o AWS CLI, execute os seguintes comandos:

     1. Crie o conjunto de alterações para a RDKlib-Layer.

        ```
        aws serverlessrepo create-cloud-formation-change-set --application-id
         arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
        stack-name RDKlib-Layer
        ```

        Ele retorna a seguinte saída:

        ```
        {
            "ApplicationId": "arn:aws:serverlessrepo:ap-
        southeast-1:711761543063:applications/rdklib",
            "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
        a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
            "SemanticVersion": "0.1.0",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
        serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
        }
        ```

     2. Execute o conjunto de alterações. Você pode copiar/colar o ARN completo do conjunto de alterações ChangeSetId (da saída gerada na etapa anterior) para personalizar o seguinte comando:

        ```
        aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
        ```

     3. Retorne todos os recursos associados que fazem parte da pilha implantada.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

Ele retorna a seguinte saída:

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copie o ARN da camada do Lambda da saída gerada na etapa anterior. O ARN da camada do Lambda é o `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. A próxima etapa é definir uma função para a função do Lambda assumir. Por padrão, as funções do Lambda tentam assumir a função `AWSServiceRoleForConfig`, o que não é permitido. Você precisa criar uma função com a política gerenciada `AWS_ConfigRole`. A função deve ter uma relação de confiança com o AWS Config e todas as funções no caminho /rdk/ devem assumi-la. Veja abaixo um exemplo de política de confiança:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

Usando essa política de confiança, execute o seguinte comando:

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Agora, execute o comando abaixo para atualizar o parâmetro de entrada para `ExecutionRoleName` e fornecer o nome da função:

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-
name"}'
```

Você também pode usar `rdk modify` para atualizar os detalhes da regra acionada por mudanças usando os seguintes sinalizadores:

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

5. A etapa final é implantar a regra. Para implantá-la, execute o seguinte comando com o ARN da camada do Lambda da etapa 3:

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. A regra agora está implantada. Você pode usar o AWS Config console para verificar se a regra está funcionando conforme o esperado.

Regras periódicas

1. Para criar uma regra que seja acionada periodicamente para um tipo de recurso especificado, execute o seguinte comando:

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-
types AWS::Resource::Type --maximum-frequency EXECUTION_FREQUENCY
```

O exemplo a seguir cria uma regra que é acionada a cada 24 horas para o tipo de recurso `AWS::IAM::User`:

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
 --maximum-frequency TwentyFour_Hours
```

A seguir estão os sinalizadores que você pode usar com o comando `rdk create` para regras periódicas:

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

> **Note**
>
> Para usar a RDKlib, o tempo de execução da regra deve ser definido como `python3.6-lib`.

Depois de executar o `rdk create`, você deve ver um novo diretório com o nome da regra e três arquivos nele:

- *RULE_NAME*`.py`: arquivo Python onde a lógica da regra é armazenada.
- *RULE_NAME*`_test.py`: arquivo Python onde os testes unitários da regra são armazenados.
- `parameters.json`: arquivo JSON para as configurações de implantação do RDK.

2. A próxima etapa é escrever a lógica da regra. Você só precisará editar o arquivo *RULE_NAME*.py. Se você abrir o arquivo *RULE_NAME*.py, verá um modelo onde poderá adicionar a lógica das regras. Veja abaixo o modelo que foi gerado para MFA_ENABLED_RULE:

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
```

```
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

O modelo usa como padrão as regras acionadas por mudanças. Em vez disso, adicione sua lógica ao método `evaluate_periodic`. O exemplo a seguir é uma versão editada do modelo MFA_ENABLED_RULE com a lógica da regra. A regra verifica se os usuários do IAM têm autenticação multifator (MFA) habilitada. A regra será NON_COMPLIANT se um usuário do IAM não tiver a MFA habilitada. Para obter mais informações sobre a lógica de regras e os métodos fornecidos no modelo, consulte Lógica da regra.

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):l

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        evaluations = []

        iam_client = client_factory.build_client("iam")

        paginator = iam_client.get_paginator("list_users")
        response_iterator = paginator.paginate()

        for response in response_iterator:
            for user in response["Users"]:
                username = user["UserName"]
                response = iam_client.list_mfa_devices(UserName=username)

                # Scenario:1 IAM user has MFA enabled.
                if response["MFADevices"]:
                    evaluations.append(Evaluation(ComplianceType.COMPLIANT,
 username, "AWS::IAM::User"))

                # Scenario:2 IAM user has MFA not enabled.
                if not response["MFADevices"]:
                    annotation = "MFA needs to be enabled for user."
                    evaluations.append(
```

```
                        Evaluation(ComplianceType.NON_COMPLIANT, username,
 "AWS::IAM::User", annotation=annotation)
                    )
        return evaluations

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. A próxima etapa é instalar a camada RDKlib AWS com o AWS console ou. AWS CLI A RDKlib foi projetada para funcionar como uma camada do AWS Lambda . Ela permite que você use a biblioteca sem precisar incluí-la no pacote de implantação.

   - Para instalar a camada RDKlib com o AWS console, siga as seguintes etapas:

     1. Abra o AWS Serverless Application Repository console em https://console.aws.amazon.com/serverlessrepo.
     2. No menu de navegação à esquerda, escolha Aplicativos disponíveis.
     3. Pesquise `rdklib` e escolha rdklib.
     4. Revise os detalhes da função e implante-a. Nenhuma alteração deve ser necessária.
     5. Na seção Recursos na página Visão geral, copie o Amazon Resource Name (ARN) da camada Lambda. Você precisará do ARN da camada do Lambda ao implantar a regra.

   - Para instalar a camada RDKlib com o AWS CLI, execute os seguintes comandos:

     1. Crie o conjunto de alterações para a RDKlib-Layer.

        ```
        aws serverlessrepo create-cloud-formation-change-set --application-id
         arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --
        stack-name RDKlib-Layer
        ```

        Ele retorna a seguinte saída:

        ```
        {
        ```

```
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. Execute o conjunto de alterações. Você pode copiar/colar o ARN completo do conjunto de alterações ChangeSetId (da saída gerada na etapa anterior) para personalizar o seguinte comando:

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. Retorne todos os recursos associados que fazem parte da pilha implantada.

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

Ele retorna a seguinte saída:

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. Copie o ARN da camada do Lambda da saída gerada na etapa anterior. O ARN da camada do Lambda é o `PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-
layer:1"
```

4. A próxima etapa é definir uma função para a função do Lambda assumir. Por padrão, as funções do Lambda tentam assumir a função `AWSServiceRoleForConfig`, o que não é permitido. Você precisa criar uma função com a política gerenciada `AWS_ConfigRole`. A função deve ter uma relação de confiança com o AWS Config e todas as funções no caminho /rdk/ devem assumi-la. Veja abaixo um exemplo de política de confiança:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

Usando essa política de confiança, execute o seguinte comando:

```
aws iam create-role --role-name your-role-name --assume-role-policy-document
 file://trust-policy.json
```

Agora, execute o comando abaixo para atualizar o parâmetro de entrada para `ExecutionRoleName` e fornecer o nome da função:

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-name"}'
```

Você também pode usar `rdk modify` para atualizar os detalhes da regra periódica usando os seguintes sinalizadores:

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a
 rule to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on
 a periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

5. A etapa final é implantar a regra. Para implantá-la, execute o seguinte comando com o ARN da camada do Lambda da etapa 3:

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. A regra agora está implantada. Você pode usar o AWS Config console para verificar se a regra está funcionando conforme o esperado.

Lógica da regra

O exemplo de código Python a seguir é um modelo para escrever uma regra usando o RDK e a RDKlib. Você só deve fazer alterações nos métodos `evaluate_parameters`, `evaluate_change` e `evaluate_periodic` ou escrever funções completamente novas para ajudar com a lógica, se necessário. Para obter os pré-requisitos para escrever regras com o RDK e a RDKLib, consulte Pré-requisitos.

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ["AWS::Resource::Type"]
```

```
# When you create a rule, the class name will be the name you give the rule when you
 create it instead of ConfigRule
class ConfigRule (ConfigRule):

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        ##############################
        # Add your custom logic here. #
        ##############################

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = ConfigRule()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

APPLICABLE_RESOURCES

`APPLICABLE_RESOURCES` são os tipos de recursos que a regra tem como alvo. Se usada, essa deve ser uma variável global definida para os tipos de recursos que a regra tem como alvo. Para obter uma lista de tipos de recursos compatíveis, consulte Supported Resource Types.

avaliar_parâmetros

Descrição

Esse método é usado para verificar se os parâmetros de entrada da regra são válidos. Veja a seguir as práticas recomendadas:

- Verifique se o número correto de parâmetros está listado.
- Verifique se o nome do parâmetro está correto.
- Verifique se o valor do parâmetro é do tipo correto.

- Se o parâmetro for um número inteiro, verifique se o parâmetro está entre limites razoáveis.
- Se o parâmetro tiver um número limitado de opções possíveis, verifique se o parâmetro é uma dessas opções.
- Se o parâmetro for uma String, verifique se ele tem um tamanho razoável e remova qualquer espaço antes ou depois do valor.
- Verifique se alguma distinção entre maiúsculas e minúsculas é tratada adequadamente.
- Limite a entrada de parâmetros quando possível. Por exemplo, se você estiver recebendo uma lista de ARNs separados por vírgulas, garanta que os únicos caracteres permitidos sejam vírgulas e os caracteres aceitos pelos ARNs.

Parâmetros

`rule_parameters` é um dicionário de parâmetros de entrada para a regra.

Sintaxe de retorno

Se um dos parâmetros não for válido, você poderá gerar um erro `InvalidParametersError`:

```
from rdklib import InvalidParametersError
raise InvalidParametersError("Error message to display")
```

Se todos os parâmetros forem válidos, o método deverá retornar um dicionário:

```
return valid_rule_parameters
```

evaluate_change

Descrição

Esse método é usado para que a lógica avalie uma regra acionada por mudanças.

Parâmetros

`event`é o AWS Lambda evento fornecido por AWS Config. É um documento no formato JSON que contém dados para uma função do Lambda operar. Para ver exemplos, consulte Exemplos de eventos para AWS Config regras.

`client_factory`é o ClientFactory objeto a ser usado para a regra. A ClientFactory classe cria ou reutiliza um cliente boto3, que fornece uma interface de baixo nível para um serviço. AWS Os métodos do cliente boto3 são mapeados com uma API de AWS serviço, o que significa que as operações de serviço são mapeadas para métodos do cliente com o mesmo nome e fornecem

acesso aos mesmos parâmetros de operação. Para obter uma lista dos serviços disponíveis, consulte Available Services na documentação do Boto3 Docs.

A sintaxe de solicitação de `client_factory` é a seguinte:

```
response = client_factory.build_client(
    service='string')
```

Por exemplo: .

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> O nome boto3 do AWS serviço é obrigatório.

`configuration_item` é o dicionário do item de configuração completo, mesmo se for muito grande. Um item de configuração representa uma point-in-time visão dos vários atributos de um AWS recurso suportado. Para obter informações sobre o conteúdo de`ConfigurationItem`, consulte ConfigurationItemna Referência AWS Config da API.

`valid_rule_parameters` é a saída do método `evaluate_parameters()`.

Sintaxe de retorno

O método deve retornar um ou mais dos seguintes:

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Os relatórios de regras sobre recursos excluídos devem retornar o resultado da avaliação de `NOT_APPLICABLE`, a fim de evitar avaliações desnecessárias de regras.

Você deve usar anotações para todas as avaliações não compatíveis. Por exemplo: .

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

evaluate_periodic

Descrição

Esse método é usado para avaliar uma regra periódica.

Parâmetros

`event`é o AWS Lambda evento fornecido por AWS Config. É um documento no formato JSON que contém dados para uma função do Lambda operar. Para ver exemplos, consulte Exemplos de eventos para AWS Config regras.

`client_factory`é o ClientFactory objeto a ser usado para a regra. A ClientFactory classe cria ou reutiliza um cliente boto3, que fornece uma interface de baixo nível para um serviço. AWS Os métodos do cliente boto3 são mapeados com uma API de AWS serviço, o que significa que as operações de serviço são mapeadas para métodos do cliente com o mesmo nome e fornecem acesso aos mesmos parâmetros de operação. Para obter uma lista dos serviços disponíveis, consulte Available Services na documentação do Boto3 Docs.

A sintaxe de solicitação de `client_factory` é a seguinte:

```
response = client_factory.build_client(
    service='string')
```

Por exemplo: .

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> O nome boto3 do AWS serviço é obrigatório.

`valid_rule_parameters` é a saída do método `evaluate_parameters()`.

Sintaxe de retorno

O método deve retornar um ou mais dos seguintes:

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

> **Note**
>
> Os relatórios de regras sobre recursos excluídos devem retornar o resultado da avaliação de `NOT_APPLICABLE`, a fim de evitar avaliações desnecessárias de regras.

Você deve usar anotações para todas as avaliações não compatíveis. Por exemplo: .

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why
 the rule is NON_COMPLIANT")]]
```

lambda_handler

Descrição

Você não precisa modificar esse método. O manipulador lambda é usado para processar eventos. A função é executada quando AWS Lambda passa o `event` objeto para o `handler` método. Para obter mais informações, consulte Manipulador de função do Lambda em Python.

Parâmetros

`event`é o AWS Lambda evento fornecido por AWS Config. É um documento no formato JSON que contém dados para uma função do Lambda operar. Para ver exemplos, consulte Exemplos de eventos para AWS Config regras.

`context` é um objeto passado para sua função pelo Lambda no runtime. Esse objeto oferece métodos e propriedades que fornecem informações e métodos que a função pode usar durante a execução. Observe que nas versões mais recentes do Lambda, o contexto não é mais usado.

Modo de avaliação e tipos de gatilho para AWS Config regras

Ao adicionar uma regra à sua conta, você pode especificar quando, no processo de criação e gerenciamento de recursos, você AWS Config deseja avaliar seus recursos. O processo de criação e gerenciamento de recursos é conhecido como provisionamento de recursos. Você escolhe o modo de avaliação para especificar quando, nesse processo, AWS Config deseja avaliar seus recursos.

Dependendo da regra, AWS Config pode avaliar suas configurações de recursos antes de um recurso ser implantado, depois de um recurso ter sido implantado ou ambos. Avaliar um recurso antes que ele seja implantado é uma avaliação proativa. Avaliar um recurso após sua implantação é uma avaliação de detecção.

Você também pode escolher o tipo de acionador para especificar com que frequência suas regras do AWS Config avaliam seus recursos. Os recursos podem ser avaliados quando há alterações na configuração, em um cronograma periódico ou em ambos.

Tipos de trigger

Depois de adicionar uma regra à sua conta, AWS Config compara seus recursos com as condições da regra. Após essa avaliação inicial, AWS Config continua executando avaliações cada vez que uma é acionada. Os triggers de avaliação são definidos como parte da regra e podem incluir os seguintes tipos:

Tipo de gatilho	Descrição
Alterações de configuração	AWS Config executa avaliações para a regra quando há um recurso que correspon de ao escopo da regra e há uma alteração na configuração do recurso. A avaliação é executada após o AWS Config envio de uma notificação de alteração do item de configura ção. Você escolhe quais recursos acionam a avaliação, definindo o escopo da regra. O escopo pode incluir o seguinte: • Um ou mais tipos de recursos

Tipo de gatilho	Descrição
	• A combinação de um tipo de recurso e um ID de recurso • A combinação de uma chave de tag e valor • Quando os recursos registrados são criados, atualizados ou excluídos AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponda ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações.
Periódico	AWS Config executa avaliações para a regra na frequência que você escolher; por exemplo, a cada 24 horas.
Híbrida	Algumas regras têm alterações na configura ção e gatilhos periódicos. Para essas regras, AWS Config avalia seus recursos quando detecta uma alteração na configuração e também na frequência que você especifica.

Modos de avaliação

Há dois modos de avaliação:

Modo proativo

Use a avaliação proativa para avaliar os recursos antes de serem implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

O Esquema do tipo de recurso indica as propriedades de um recurso. Você pode encontrar o esquema do tipo de recurso em "extensões AWS públicas" no AWS CloudFormation registro ou com o seguinte comando da CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obter mais informações, consulte Gerenciamento de extensões por meio do AWS CloudFormation registro e da referência de tipos de AWS recursos e propriedades no Guia AWS CloudFormation do usuário.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Lista de regras gerenciadas com avaliação proativa

Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

Lista de tipos de recursos compatíveis para avaliação proativa

Apresentamos uma lista dos tipos de recursos que são compatíveis com a avaliação proativa:

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

Exemplo de regra com avaliação proativa

Exemplo de regra proativa

1. Você adiciona a regra AWS Config gerenciada,`S3_BUCKET_LOGGING_ENABLED`, à sua conta para verificar se seus buckets do S3 têm o registro ativado.
2. Para o modo de avaliação, escolha Ativar avaliação proativa no AWS Management Console ou habilitar `PROACTIVE` para `EvaluationModes` na PutConfigRuleAPI.

Depois de ativar a avaliação proativa, você pode usar a StartResourceEvaluationAPI e a GetResourceEvaluationSummaryAPI para verificar se um bucket em sua conta, que não foi implantado na produção, não tem o registro ativado. Isso permite que você teste as configurações dos recursos antes da implantação e reavalie se quiser implantar o recurso na produção.

Por exemplo, comece com a StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::S3::Bucket",
                                     "ResourceConfiguration": "{\"BucketName\": \"my-
bucket\", \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Você deve receber o `ResourceEvaluationId` na saída:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Em seguida, use o `ResourceEvaluationId` com a GetResourceEvaluationSummary API para verificar o resultado da avaliação:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Você deve receber uma saída semelhante à seguinte:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration": "{\"BucketName\": \"my-bucket\",
 \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

    }
}
```

Para ver informações adicionais sobre o resultado da avaliação, como qual regra sinalizou um recurso como NON_COMPLIANT, use a API. GetComplianceDetailsByResource

Modo de detecção

Use a avaliação de detecção para avaliar os recursos que já foram implantados. Isso permite avaliar as definições de configuração de seus recursos existentes.

Exemplos de regras com avaliação de detecção

Exemplo de regra acionada por alterações

1. Você adiciona a regra gerenciada, `S3_BUCKET_LOGGING_ENABLED`, à sua conta para verificar se seus buckets do S3 têm o registro em log habilitado.
2. O tipo de gatilho para a regra são as alterações de configuração. AWS Config executa as avaliações da regra quando um bucket do S3 é criado, alterado ou excluído.
3. Quando um bucket é atualizado, a alteração de configuração aciona a regra e o AWS Config avalia se o bucket é compatível com a regra.

Exemplo de regra periódica

1. Você adiciona a regra gerenciada, `IAM_PASSWORD_POLICY`, à sua conta. A regra verifica se a política de senha para seus usuários do IAM é compatível com a política de sua conta, como a exigência de um tamanho mínimo ou de caracteres específicos.
2. O tipo de acionador da regra é periódico. AWS Config executa a avaliação da regra na frequência especificada por você, como a cada 24 horas.
3. A cada 24 horas, a regra é iniciada e AWS Config avalia se as senhas dos usuários do IAM estão em conformidade com a regra.

Exemplo de regra híbrida com triggers de alteração de configuração e periódico

1. Crie uma regra personalizada que avalie se as AWS CloudTrail trilhas em sua conta estão ativadas e registradas em todas as regiões.
2. Você AWS Config deseja executar avaliações para a regra sempre que uma trilha for criada, atualizada ou excluída. Você também quer AWS Config executar a regra a cada 12 horas.
3. Para o tipo de acionador, você grava a lógica tanto para a alteração da configuração quanto para os acionadores periódicos. Para obter mais informações, consulte Componentes de uma AWS Config regra: escrevendo regras.

Avaliações de regras quando o gravador de configuração está desativado

Se você desligar o gravador de configuração, AWS Config interromperá o registro das alterações nas configurações dos recursos. Isso afeta suas avaliações de regras da seguinte forma:

- Regras com um trigger periódico continuam a executar avaliações na frequência especificada.
- As regras acionadas por alterações não executam avaliações.
- As regras híbridas executam avaliações somente na frequência especificada. As regras não executam avaliações para alterações de configuração.
- Se você executa uma avaliação sob demanda para uma regra com um trigger de alteração de configuração, a regra avalia o último estado conhecido do recurso, que é o último item de configuração gravado.

> **Important**
>
> Evite AWS Config avaliações desnecessárias
>
> As regras periódicas e as regras híbridas continuarão em execução, a menos que sejam excluídas, mesmo que você tenha desativado o gravador de configuração. Essas regras avaliarão somente os itens de configuração que foram gravados antes de o gravador de configuração ser desativado, o que significa que essas regras reproduzirão os mesmos resultados da avaliação, sem novas informações. Exclua regras periódicas e regras híbridas ao desabilitar o gravador de configuração para evitar atividades desnecessárias e avaliações de regras.

AWS Config Regras gerenciadas

AWS Config fornece regras AWS gerenciadas, que são regras predefinidas e personalizáveis AWS Config usadas para avaliar se seus AWS recursos estão em conformidade com as melhores práticas comuns. Por exemplo, você pode usar uma regra gerenciada para começar rapidamente a avaliar se os seus volumes do Amazon Elastic Block Store (Amazon EBS) são criptografados ou se tags específicas são aplicadas a seus recursos. O AWS Config console orienta você pelo processo de configuração e ativação de uma regra gerenciada. Você também pode usar a AWS Config API AWS Command Line Interface ou para transmitir o código JSON que define sua configuração de uma regra gerenciada.

Você pode personalizar o comportamento de uma regra gerenciada para atender às suas necessidades. Por exemplo, você pode definir o escopo da regra para restringir quais recursos acionam uma avaliação para a regra, como instâncias ou volumes do EC2. Você pode personalizar os parâmetros da regra para definir atributos que seus recursos devem ter para ser compatíveis com a regra. Por exemplo, você pode personalizar um parâmetro para especificar que o seu grupo de segurança deve bloquear o tráfego de entrada para um número de porta específico.

Considerações sobre custos

Para obter detalhes sobre os custos associados ao registro de recursos, consulte AWS Config preços.

Recomendação: pare de registrar a conformidade dos recursos antes de excluir as regras

É altamente recomendável que você interrompa a gravação do tipo de `AWS::Config::ResourceCompliance` recurso antes de excluir as regras da sua conta. A

exclusão de regras cria itens de configuração (CIs) `AWS::Config::ResourceCompliance` e pode afetar os custos do gravador AWS Config de configuração. Se você estiver excluindo regras que avaliam um grande número de tipos de recursos, isso pode levar a um aumento no número de ICs registrados.

Melhor prática:

1. Pare de gravar `AWS::Config::ResourceCompliance`
2. Excluir regra (s)
3. Ativar a gravação para `AWS::Config::ResourceCompliance`

Tipos de trigger

Depois de adicionar uma regra à sua conta, AWS Config compara seus recursos com as condições da regra. Após essa avaliação inicial, AWS Config continua executando avaliações cada vez que uma é acionada. Os acionadores de avaliação são definidos como parte da regra e podem incluir os seguintes tipos.

Tipo de gatilho	Descrição
Alterações de configuração	AWS Config executa avaliações para a regra quando há um recurso que correspon de ao escopo da regra e há uma alteração na configuração do recurso. A avaliação é executada após o AWS Config envio de uma notificação de alteração do item de configura ção. Você escolhe quais recursos acionam a avaliação, definindo o escopo da regra. O escopo pode incluir o seguinte: • Um ou mais tipos de recursos • A combinação de um tipo de recurso e um ID de recurso •

Tipo de gatilho	Descrição
	• A combinação de uma chave de tag e valor • Quando os recursos registrados são criados, atualizados ou excluídos AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponde ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações.
Periódico	AWS Config executa avaliações para a regra na frequência que você escolher; por exemplo, a cada 24 horas.
Híbrida	Algumas regras têm alterações na configura ção e gatilhos periódicos. Para essas regras, AWS Config avalia seus recursos ao detectar uma alteração na configuração e também na frequência especificada.

Modos de avaliação

Há dois modos de avaliação das AWS Config regras.

Modo de avaliação	Descrição
Proativo	Use a avaliação proativa para avaliar os recursos antes de serem implantados. Isso permite avaliar se um conjunto de proprieda des de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de

Modo de avaliação	Descrição
	regras proativas que você tem em sua conta na sua região. Para obter mais informações, consulte Modos de avaliação. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.
Detecção	Use a avaliação de detecção para avaliar os recursos que já foram implantados. Isso permite avaliar as definições de configuração de seus recursos existentes.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Tópicos

- Lista de regras AWS Config gerenciadas
- Lista de regras AWS Config gerenciadas por modo de avaliação
- Lista de regras AWS Config gerenciadas por tipo de acionador
- Disponibilidade da lista de regras AWS Config gerenciadas por região
- Regras vinculadas ao serviço AWS Config
- Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation

Lista de regras AWS Config gerenciadas

AWS Config atualmente oferece suporte às seguintes regras gerenciadas.

Considerações

Valores padrão para regras gerenciadas

Os valores padrão especificados para regras gerenciadas são pré-preenchidos somente ao usar o AWS console. Os valores padrão não são fornecidos para a API, a CLI ou o SDK.

Não há suporte para buckets de diretório

As regras gerenciadas só oferecem suporte a buckets de uso geral ao avaliar os recursos do Amazon Simple Storage Service (Amazon S3). AWS Config não registra alterações de configuração para buckets de diretório. Para obter mais informações sobre buckets de uso geral e buckets de diretório, consulte Visão geral dos buckets e Buckets de diretório no Guia do usuário do Amazon S3.

Regras gerenciadas e tipos de recursos globais do IAM

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Tópicos

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-

- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer ativado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- verificação de expiração do certificado do servidor iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

access-keys-rotated

Verifica se as chaves de acesso ativas são alternadas (alteradas) dentro do número de dias especificado em `maxAccessKeyAge`. A regra será NON_COMPLIANT se as chaves de acesso não forem alternadas dentro do período especificado. O valor padrão é 90 dias.

> **Warning**
>
> Não as forneça a terceiros não autorizados, mesmo que seja para ajudar a localizar os identificadores da sua conta. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta. As melhores práticas de segurança são remover senhas e chaves de acesso quando os usuários não precisam mais delas.

> **Note**
>
> Tipo de recurso marcado como não compatível no console
> Se essa regra constatar que alguma de suas chaves de acesso não está em conformidade, o tipo de `AWS::IAM::User` recurso também será marcado como não compatível no console. AWS
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
> Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
> Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para

obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.
Limitações
Essa regra não se aplica às chaves de acesso do usuário raiz da AWS conta. Para excluir ou alternar suas chaves de acesso de usuário raiz, use suas credenciais de usuário raiz para entrar na página Minhas Credenciais de Segurança no endereço. AWS Management Console https://aws.amazon.com/console/

Identifier (Identificador): ACCESS_KEYS_ROTATED

Tipos de recursos: AWS::IAM::User

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

AccessKeyIdade máxima, Tipo: int, Padrão: 90

Número máximo de dias sem alternância. Padrão 90.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

account-part-of-organizations

Verifica se uma AWS conta faz parte do AWS Organizations. A regra é NON_COMPLIANT se uma AWS conta não fizer parte do Organizations AWS ou se o ID da conta principal do AWS Organizations não corresponder ao parâmetro da regra. `MasterAccountId`

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados

nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identificador: ACCOUNT_PART_OF_ORGANIZATIONS

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

MasterAccountId (Opcional), Tipo: string

O ID da conta principal de uma AWS conta.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

acm-certificate-expiration-check

Verifica se os certificados do AWS Certificate Manager em sua conta estão marcados para expiração dentro do número de dias especificado. Os certificados fornecidos pelo ACM são renovados automaticamente. O ACM não renova automaticamente os certificados que você importar. A regra será NON_COMPLIANT se seus certificados estiverem prestes a expirar.

Identifier (Identificador): ACM_CERTIFICATE_EXPIRATION_CHECK

Tipos de recursos: AWS::ACM::Certificate

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

daysToExpiration (Opcional), Tipo: int, Padrão: 14

Especifique o número de dias antes de a regra sinalizar o Certificado ACM como não compatível.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

acm-certificate-rsa-check

Verifica se os certificados RSA gerenciados pelo AWS Certificate Manager (ACM) têm um tamanho de chave de pelo menos '2048' bits. A regra não é compatível se o tamanho mínimo da chave for menor que 2048 bits.

Identificador: ACM_CERTIFICATE_RSA_CHECK

Tipos de recursos: AWS::ACM::Certificate

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

acm-pca-root-ca-disabled

Verifica se a Autoridade de Certificação AWS AWS Privada (CA Privada) tem uma CA raiz que está desativada. A regra é NON_COMPLIANT para CAs raiz com status que não é DISABLED.

Identificador: ACM_PCA_ROOT_CA_DISABLED

Tipos de recursos: AWS::ACMPCA::CertificateAuthority

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

exemptedCAArns (opcional), Tipo: Csv

> Lista separada por vírgulas de nomes do recurso da Amazon (ARNs) de ACs que podem ser habilitados. Esse valor pode ser fornecido para outras CAs, como CAs raiz específicas ou CAs intermediárias que podem ser habilitadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

alb-desync-mode-check

Verifica se um Application Load Balancer (ALB) está configurado com um modo de mitigação de dessincronização definido pelo usuário. A regra será NON_COMPLIANT se o modo de mitigação de dessincronização ALB não corresponder ao modo de mitigação de dessincronização definido pelo usuário.

Identificador: ALB_DESYNC_MODE_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

desyncMode, Tipo: Csv

> Lista separada por vírgulas, na qual os clientes podem escolher no máximo dois valores entre: 'defensivo', 'mais rigoroso' e 'monitor'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

alb-http-drop-invalid-header-enabled

Verifica se a regra avalia os AWS Application Load Balancers (ALB) para garantir que eles estejam configurados para descartar cabeçalhos http. A regra não é compatível se o valor de routing.http.drop_invalid_header_fields.enabled estiver definido como falso.

Identificador: ALB_HTTP_DROP_INVALID_HEADER_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

alb-http-to-https-redirection-check

Verifica se o redirecionamento de HTTP para HTTPS está configurado em todos os receptores HTTP do Application Load Balancers. A regra será NON_COMPLIANT se um ou mais receptores HTTP do Application Load Balancer não tiverem o redirecionamento HTTP para HTTPS configurado. A regra também é NON_COMPLIANT se um ou mais receptores de HTTP tiver encaminhamento para um receptor de HTTP, em vez de redirecionamento.

Identifier (Identificador): ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

alb-waf-enabled

Verifica se o AWS WAF está habilitado nos Application Load Balancers (ALBs). A regra será NON_COMPLIANT se a chave: waf.enabled estiver definida como falsa.

Identificador: ALB_WAF_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

waf WebAclIds (opcional), Tipo: Csv

> Lista separada por vírgulas do ID da ACL da web (para WAF) ou do ARN da ACL da web (para WAFV2) verificando a associação do ALB.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gwv2-access-logs-enabled

Verifica se os estágios do Amazon API Gateway V2 têm o registro em log de acesso habilitado. A regra é NON_COMPLIANT se o LogSettings 'acesso' não estiver presente na configuração do Stage.

Identificador: API_GWV2_ACCESS_LOGS_ENABLED

Tipos de recursos: AWS::ApiGatewayV2::Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gwv2-authorization-type-configured

Verifica se as rotas de API do Amazon API Gatewayv2 têm um tipo de autorização definido. Essa regra será NON_COMPLIANT se o tipo de autorização for NONE.

Identificador: API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

Tipos de recursos: AWS::ApiGatewayV2::Route

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

authorizationType (opcional), Tipo: string

> Parâmetro para comparar os tipos de autorização das rotas de API. Os parâmetros de string correspondentes a CUSTOM, AWS_IAM, JWT são válidos.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gw-associated-with-waf

Verifica se um estágio de API do Amazon API Gateway está usando uma lista de controle de acesso à web do AWS WAF (web ACL). A regra é NON_COMPLIANT se uma AWS WAF Web ACL não for usada ou se uma AWS Web ACL usada não corresponder ao que está listado no parâmetro da regra.

Identificador: API_GW_ASSOCIATED_WITH_WAF

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

WebAclArns (Opcional), Tipo: Csv

Lista separada por vírgulas dos Nomes de recursos da Amazon (ARNs) da ACL da web.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

api-gw-cache-enabled-and-encrypted

Verifica se todos os métodos nos estágios do Amazon API Gateway têm o cache habilitado e o cache criptografado. A regra será NON_COMPLIANT se qualquer método em um estágio do Amazon API Gateway não estiver configurado para armazenamento em cache ou se o cache não estiver criptografado.

Identifier (Identificador): API_GW_CACHE_ENABLED_AND_ENCRYPTED

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gw-endpoint-type-check

Verifica se as APIs do Amazon API Gateway são do tipo especificado no parâmetro `endpointConfigurationType` da regra. A regra retornará NON_COMPLIANT se a API REST não corresponder ao tipo de endpoint configurado no parâmetro da regra.

Identifier (Identificador): API_GW_ENDPOINT_TYPE_CHECK

Tipos de recursos: AWS::ApiGateway::RestApi

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

ponto final ConfigurationTypes, Tipo: string

> Lista separada por vírgula dos permitidos. endpointConfigurationTypes Os valores permitidos são REGIONAL, PRIVATE e EDGE.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gw-execution-logging-enabled

Verifica se todos os métodos no estágio do Amazon API Gateway têm o registro em log habilitado. A regra será NON_COMPLIANT se o registro em log não estiver habilitado, ou se `loggingLevel` não for ERROR nem INFO.

Identifier (Identificador): API_GW_EXECUTION_LOGGING_ENABLED

Tipos de recursos: AWS::ApiGateway::Stage, AWS::ApiGateway V2: :Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

loggingLevel (opcional), Tipo: string, Padrão: ERROR, INFO

Lista separada por vírgulas de níveis de registro em log específicos (por exemplo, ERROR, INFO ou ERROR,INFO).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gw-ssl-enabled

Verifica se um estágio da API REST usa um certificado SSL. A regra será NON_COMPLIANT se o estágio da API REST não tiver um certificado SSL associado.

> **Note**
>
> Essa regra será retornada `NOT_APPLICABLE` se a GetIntegrationAPI retornar `AWS` como tipo.

Identificador: API_GW_SSL_ENABLED

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

CertificateIDs (opcional), Tipo: Csv

Lista separada por vírgulas de IDs de certificados de clientes configurados em um estágio da API REST.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

api-gw-xray-enabled

Verifica se o rastreamento de AWS X-Ray está ativado nas APIs REST do Amazon API Gateway. A regra será COMPLIANT se o rastreamento do X-Ray estiver habilitado e, caso contrário, será NON_COMPLIANT.

Identificador: API_GW_XRAY_ENABLED

Tipos de recursos: AWS::ApiGateway::Stage

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

approved-amis-by-id

Verifica se as instâncias EC2 em execução estão usando imagens de máquina da Amazon (AMIs) especificadas. Especifique uma lista de IDs de AMI aprovadas. Instâncias em execução com AMIs que não estão nessa lista são NON_COMPLIANT.

Identifier (Identificador): APPROVED_AMIS_BY_ID

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

amiIds, Tipo: Csv

> Os IDs de AMI (lista separada por vírgulas de até 21 IDs de AMI ou 1.024 caracteres no total, o que ocorrer primeiro).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

approved-amis-by-tag

Verifica se instâncias em execução estão usando imagens de máquina da Amazon (AMIs) especificadas. Especifique as tags que identificam os AMIs. Instâncias em execução com AMIs que não têm pelo menos uma das tags especificadas são NON_COMPLIANT.

Identifier (Identificador): APPROVED_AMIS_BY_TAG

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Valor dos alvos ByTag KeyAnd, Tipo: StringMap, Padrão: tag-key:tag-value,other-tag-key

> As AMIs por tag (lista separada por vírgulas de até 10; por exemplo,`tag-key:tag-value`; ou seja, `tag-key1` combina AMIs com `tag-key1`, `tag-key2:value2` corresponde `tag-key2` com valor2).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

appsync-associated-with-waf

Verifica se as AWS AppSync APIs estão associadas às listas de controle de acesso à web AWS (ACLs) do WAFv2. A regra é NON_COMPLIANT para uma AWS AppSync API se não estiver associada a uma ACL da web.

Identificador: APPSYNC_ASSOCIATED_WITH_WAF

Tipos de recursos: AWS::AppSync::Graph QLAPI

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

waf WebAcl ARNs (opcional), Tipo: Csv

> Lista separada por vírgulas de nomes do recurso da Amazon (ARNs) para ACLs da web autorizadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

appsync-authorization-check

Verifica se uma AWS AppSync API está usando mecanismos de autorização permitidos. A regra será NON_COMPLIANT se um mecanismo de autorização não aprovado estiver sendo usado.

Identificador: APPSYNC_AUTHORIZATION_CHECK

Tipos de recursos: AWS::AppSync::Graph QLAPI

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

AllowedAuthorizationTipos, Tipo: Csv

> Lista separada por vírgula dos mecanismos de AWS AppSync autorização permitidos. Os valores permitidos são: 'API_KEY', 'AWS_LAMBDA', 'AWS_IAM', 'OPENID_CONNECT', 'AMAZON_COGNITO_USER_POOLS'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

appsync-cache-encryption-at-rest

Verifica se um cache de AWS AppSync API tem a criptografia em repouso ativada. Essa regra é NON_COMPLIANT se 'AtRestEncryptionEnabled' for falsa.

Identificador: APPSYNC_CACHE_ENCRYPTION_AT_REST

Tipos de recursos: AWS::AppSync::Graph QLAPI

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

appsync-logging-enabled

Verifica se uma AWS AppSync API tem o registro ativado. A regra é NON_COMPLIANT se o registro não estiver habilitado ou se o LogLevel 'campo' não for ERROR nem ALL.

Identificador: APPSYNC_LOGGING_ENABLED

Tipos de recursos: AWS::AppSync::Graph QLAPI

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

fieldLoggingLevel (Opcional), Tipo: Csv

> Lista separada por vírgulas de níveis específicos de registro em log de campo (por exemplo, ERROR, ALL).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

athena-workgroup-encrypted-at-rest

Verifica se um grupo de trabalho do Amazon Athena está criptografado em repouso. A regra será NON_COMPLIANT se a criptografia de dados em repouso não estiver habilitada para um grupo de trabalho do Athena.

Identificador: ATHENA_WORKGROUP_ENCRYPTED_AT_REST

Tipos de recursos: AWS::Athena::WorkGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

aurora-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para clusters de banco de dados Amazon Aurora. A regra será NON_COMPLIANT se o cluster de banco de dados do Amazon Relational Database Service (Amazon RDS) não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::RDS::DBCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos clusters de banco de dados do Aurora para verificação da regra, no formato `{"tagkey" : "tagValue"}` do JSON.

resourceId (opcional), Tipo: string

ID do cluster de banco de dados do Aurora para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

aurora-meets-restore-time-target

Confere se o tempo de restauração dos clusters de banco de dados do Amazon Aurora atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes um cluster de banco de dados Aurora for maior que minutos. maxRestoreTime

Identificador: AURORA_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::RDS::DBCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags dos clusters de banco de dados do Aurora para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID do cluster de banco de dados do Aurora para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

aurora-mysql-backtracking-enabled

Verifica se um cluster do Amazon Aurora MySQL tem o retrocesso habilitado. A regra será NON_COMPLIANT se o cluster do Aurora usar MySQL e não tiver o retrocesso habilitado.

Identificador: AURORA_MYSQL_BACKTRACKING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Disponível somente na Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Canadá (Central), China (Ningxia), Europa Região (Zurique)

Parâmetros:

BacktrackWindowInHours (Opcional), Tipo: double

Quantidade de tempo em horas (até 72) para retroceder o cluster do Aurora MySQL.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

aurora-resources-protected-by-backup-plan

Verifica se os clusters de banco de dados do Amazon Aurora estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o cluster de banco de dados do Amazon Relational Database Service (Amazon RDS) não estiver protegido por um plano de backup.

Identificador: AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos clusters de banco de dados do Aurora para verificação da regra, no formato `{"tagkey" : "tagValue"}` do JSON.

resourceId (opcional), Tipo: string

ID do cluster de banco de dados do Aurora para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

autoscaling-capacity-rebalancing

Verifica se o Rebalanceamento de capacidade está habilitado para grupos do Amazon EC2 Auto Scaling que usam vários tipos de instância. A regra será NON_COMPLIANT se o Rebalanceamento de capacidade não estiver habilitado.

Identificador: AUTOSCALING_CAPACITY_REBALANCING

Tipos de recursos: AWS::AutoScaling::AutoScaling Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-group-elb-healthcheck-required

Verifica se seus grupos do Amazon EC2 Auto Scaling associados a um Elastic Load Balancer usam as verificações de saúde do Elastic Load Balancing. A regra será NON_COMPLIANT se os grupos do Amazon EC2 Auto Scaling não estiverem usando verificações de integridade do Elastic Load Balancing.

Identifier (Identificador): AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Tipos de recursos: AWS::AutoScaling::AutoScaling Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o

esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-
balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*Os valores válidos são `EC2` (padrão), `ELB` e `VPC_LATTICE`. O tipo de verificação de integridade do `VPC_LATTICE` é reservado pra uso com o VPC Lattice, que está em uma versão pré-lançamento e está sujeita a alterações. Para obter mais informações, consulte Verificações de integridade de instâncias do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-launchconfig-requires-imdsv2

Verifica se somente o IMDSv2 está habilitado. Essa regra será NON_COMPLIANT se a versão de metadados não estiver incluída na configuração de execução ou se os metadados V1 e V2 estiverem habilitados.

Identificador: AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-launch-config-hop-limit

Verifica o número de saltos de rede que o token de metadados pode percorrer. Essa regra será NON_COMPLIANT se o limite de salto de resposta de metadados for maior que 1.

Identificador: AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-launch-config-public-ip-disabled

Verifica se os grupos do Amazon EC2 Auto Scaling têm endereços IP públicos habilitados por meio das configurações de execução. A regra é NON_COMPLIANT se a configuração de lançamento de um grupo do Amazon EC2 Auto Scaling estiver definida como “verdadeira”. AssociatePublicIpAddress

Identificador: AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::AutoScaling::LaunchConfiguration

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-launch-template

Verifica se um grupo do Auto Scaling do Amazon Elastic Compute Cloud (EC2) foi criado a partir de um modelo de execução do EC2. A regra será NON_COMPLIANT se o grupo de escalabilidade não for criado a partir de um modelo de execução do EC2.

Identificador: AUTOSCALING_LAUNCH_TEMPLATE

Tipos de recursos: AWS::AutoScaling::AutoScaling Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-multiple-az

Verifica se o grupo do Auto Scaling abrange várias zonas de disponibilidade. A regra será NON_COMPLIANT se o grupo do Auto Scaling não abranger várias zonas de disponibilidade.

Identificador: AUTOSCALING_MULTIPLE_AZ

Tipos de recursos: AWS::AutoScaling::AutoScaling Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo de zonas de disponibilidade esperadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

autoscaling-multiple-instance-types

Verifica se um grupo do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling usa vários tipos de instância. Essa regra será NON_COMPLIANT se o grupo do Amazon EC2 Auto Scaling tiver apenas um tipo de instância definido.

Identificador: AUTOSCALING_MULTIPLE_INSTANCE_TYPES

Tipos de recursos: AWS::AutoScaling::AutoScaling Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

backup-plan-min-frequency-and-min-retention-check

Verifica se um plano de backup tem uma regra de backup que satisfaça a frequência e o período de retenção necessários. A regra será NON_COMPLIANT se os pontos de recuperação não forem criados pelo menos com a frequência especificada ou expirarem antes do período especificado.

Identificador: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

Tipos de recursos: AWS::Backup::BackupPlan

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

requiredFrequencyValue (Opcional), Tipo: int, Padrão: 1

Valor numérico da frequência de backup necessária. Máximo de 24 por horas, 31 por dias.

requiredRetentionDays (Opcional), Tipo: int, Padrão: 35

O período de retenção obrigatório em dias.

requiredFrequencyUnit (Opcional), Tipo: string, Padrão: dias

Unidade de tempo para a frequência de backup necessária. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

backup-recovery-point-encrypted

Verifica se um ponto de recuperação está criptografado. A regra será NON_COMPLIANT se o ponto de recuperação não estiver criptografado.

Identificador: BACKUP_RECOVERY_POINT_ENCRYPTED

Tipos de recursos: AWS::Backup::RecoveryPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

backup-recovery-point-manual-deletion-disabled

Verifica se um cofre de backup tem uma política baseada em recursos vinculada que impede a exclusão de pontos de recuperação. A regra não é compatível se o Backup Vault não tiver políticas baseadas em recursos ou tiver políticas sem uma declaração 'Negar' adequada (declaração com permissões de backup: DeleteRecovery Ponto, backup: e backup: UpdateRecoveryPointLifecycle). PutBackupVaultAccessPolicy

Identificador: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

Tipos de recursos: AWS::Backup::BackupVault

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

principalArnList (Opcional), Tipo: Csv

> Lista separada por vírgula de AWS Identity and Access Management (IAM) Amazon Resource Names (ARNs) para a regra NÃO verificar.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

backup-recovery-point-minimum-retention-check

Verifica se um ponto de recuperação não expira antes do período especificado. A regra será NON_COMPLIANT se o ponto de recuperação tiver um ponto de retenção menor que o período de retenção exigido.

Identificador: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

Tipos de recursos: AWS::Backup::RecoveryPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

requiredRetentionDays (Opcional), Tipo: int, Padrão: 35

O período de retenção obrigatório em dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

beanstalk-enhanced-health-reporting-enabled

Verifica se um ambiente do AWS Elastic Beanstalk está configurado para relatórios de integridade aprimorados. A regra será COMPLIANT se o ambiente estiver configurado para relatórios de integridade aprimorados. A regra será NON_COMPLIANT se o ambiente estiver configurado para relatórios básicos de integridade.

Identificador: BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

clb-desync-mode-check

Verifica se os Classic Load Balancers (CLB) estão configurados com um modo de mitigação de dessincronização definido pelo usuário. A regra será NON_COMPLIANT se o modo de mitigação de dessincronização de CLB não corresponder ao modo de mitigação de dessincronização definido pelo usuário.

Identificador: CLB_DESYNC_MODE_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

desyncMode, Tipo: Csv

> Lista de valores separados por vírgula. Você pode selecionar no máximo dois. Os valores válidos incluem 'Defensivo', 'Mais restrito' e 'Monitor'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

clb-multiple-az

Verifica se um Classic Load Balancer abrange várias zonas de disponibilidade (AZs). A regra será NON_COMPLIANT se um Classic Load Balancer abranger menos de dois AZs ou não abranger o número de AZs mencionado no parâmetro `minAvailabilityZones` (se fornecido).

Identificador: CLB_MULTIPLE_AZ

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo desejado de AZs esperados. Os valores válidos estão entre dois e dez, ambos inclusive. O valor padrão será 2 se o parâmetro não for especificado.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudformation-stack-drift-detection-check

Verifica se a configuração real de uma pilha AWS CloudFormation (AWS CloudFormation) difere ou se desviou da configuração esperada. Considera-se que uma pilha se desviou de sua configuração se um ou mais recursos diferirem da configuração esperada. A regra e a pilha são COMPLIANT quando o status da pilha é IN_SYNC. A regra será NON_COMPLIANT se o status de desvio da pilha for DRIFTED.

> **Note**
>
> Essa regra executa a DetectStackDrift operação em cada pilha da sua conta. A DetectStackDrift operação pode levar vários minutos, dependendo do número de recursos contidos na pilha. Como o tempo máximo de execução dessa regra é limitado a 15 minutos, é possível que a regra expire antes de concluir a avaliação de todas as pilhas em sua conta. Se esse problema ocorrer, é recomendável que você restrinja o número de pilhas no escopo da regra usando tags. Você pode fazer o seguinte:
>
> 1. Divida suas pilhas em grupos, usando uma tag diferente para cada grupo.
> 2. Aplique a mesma tag a todas as pilhas desse grupo.
> 3. Inclua várias instâncias dessa regra em sua conta, cada uma delimitada por uma tag diferente. Fazer isso permite que cada instância da regra processe somente as pilhas que têm a tag correspondente mencionada em seu escopo.

Identifier (Identificador): CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

formação de nuvens RoleArn, Tipo: string

O Amazon Resource Name (ARN) da função do IAM com permissões de política para detectar desvios nas pilhas. AWS CloudFormation Para obter informações sobre as permissões necessárias do IAM para a função, consulte Detecção de alterações de configuração não gerenciadas em pilhas e recursos | Considerações ao detectar desvios no Guia do usuário. AWS CloudFormation

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudformation-stack-notification-check

Verifica se suas CloudFormation pilhas enviam notificações de eventos para um tópico do Amazon SNS. Há também a opção de verificar se os tópicos do Amazon SNS estão sendo usados. A regra é NON_COMPLIANT se as CloudFormation pilhas não enviarem notificações.

Identifier (Identificador): CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Tipos de recursos: AWS::CloudFormation::Stack

Tipo de trigger: alterações da configuração

Região da AWS: Disponível somente na China (Pequim), Ásia-Pacífico (Mumbai), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Canadá (Central), Região da China (Ningxia)

Parâmetros:

snsTopic1 (opcional), Tipo: string

ARN do tópico do SNS.

snsTopic2 (opcional), Tipo: string

ARN do tópico do SNS.

snsTopic3 (opcional), Tipo: string

ARN do tópico do SNS.

snsTopic4 (opcional), Tipo: string

ARN do tópico do SNS.

snsTopic5 (opcional), Tipo: string

ARN do tópico do SNS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-accesslogs-enabled

Verifica se CloudFront as distribuições da Amazon estão configuradas para entregar registros de acesso a um bucket do Amazon S3. A regra é NON_COMPLIANT se uma CloudFront distribuição não tiver o registro configurado.

Identificador: CLOUDFRONT_ACCESSLOGS_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

S3 BucketName (opcional), Tipo: string

O nome do bucket do Amazon S3 para armazenar logs de acesso do servidor.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-associated-with-waf

Verifica se CloudFront as distribuições da Amazon estão associadas ao firewall de aplicativos web (WAF) ou às listas de controle de acesso à web (ACLs) do WAFv2. A regra é NON_COMPLIANT se uma CloudFront distribuição não estiver associada a uma Web ACL do WAF.

Identificador: CLOUDFRONT_ASSOCIATED_WITH_WAF

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

waf WebAclIds (opcional), Tipo: Csv

> Lista separada por vírgulas de IDs de ACL da web para nomes do recurso da Amazon (ARNs) da ACL da web ou de WAF para WAFV2.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

cloudfront-custom-ssl-certificate

Verifica se o certificado associado a uma CloudFront distribuição da Amazon é o certificado SSL padrão. A regra é NON_COMPLIANT se uma CloudFront distribuição usar o certificado SSL padrão.

Identificador: CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-default-root-object-configured

Verifica se uma CloudFront distribuição da Amazon está configurada para retornar um objeto específico que é o objeto raiz padrão. A regra é NON_COMPLIANT se a CloudFront distribuição da Amazon não tiver um objeto raiz padrão configurado.

Identificador: CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-no-deprecated-ssl-protocols

Verifica se CloudFront as distribuições estão usando protocolos SSL obsoletos para comunicação HTTPS entre pontos de CloudFront presença e origens personalizadas. Essa regra é NON_COMPLIANT para uma CloudFront distribuição se algum 'OriginSslProtocolo' incluir 'SSLv3'.

Identificador: CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-origin-access-identity-enabled

Verifica se a CloudFront distribuição com o tipo de origem do Amazon S3 tem a identidade de acesso de origem configurada. A regra é NON_COMPLIANT se a CloudFront distribuição for apoiada pelo S3 e qualquer tipo de origem não estiver configurado pelo OAI ou se a origem não for um bucket do S3.

> **Note**
>
> A regra não retornará NOT_APPLICABLE se a origem não for um bucket do S3.

Identificador: CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-origin-failover-enabled

Verifica se um grupo de origem está configurado para a distribuição de pelo menos duas origens no grupo de origem da Amazon CloudFront. A regra será NON_COMPLIANT se não houver grupos de origem para a distribuição.

Identificador: CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-s3-origin-access-control-enabled

Verifica se uma CloudFront distribuição da Amazon com um tipo de origem do Amazon Simple Storage Service (Amazon S3) tem o controle de acesso de origem (OAC) ativado. A regra é NON_COMPLIANT para CloudFront distribuições com origens do Amazon S3 que não têm o OAC habilitado.

Identificador: CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-s3-origin-non-existent-bucket

Verifica se CloudFront as distribuições da Amazon apontam para um bucket S3 inexistente. A regra é NON_COMPLIANT se OriginConfig `S3` para uma CloudFront distribuição aponta para um bucket S3 inexistente. A regra não avalia buckets do S3 com hospedagem estática de sites.

Identificador: CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

Tipos de recursos: AWS::CloudFront::Distribution

Trigger type (Tipo de trigger): periódico

Região da AWS: disponível somente nas regiões da China (Pequim) e do Leste dos EUA (Norte da Virgínia).

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

cloudfront-security-policy-check

Verifica se CloudFront as distribuições da Amazon estão usando uma política de segurança mínima e um conjunto de criptografia de TLSv1.2 ou superior para conexões de visualizadores. Essa regra não é compatível para uma CloudFront distribuição se estiver abaixo de TLSv1.2_2018 minimumProtocolVersion .

Identificador: CLOUDFRONT_SECURITY_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-sni-enabled

Verifica se CloudFront as distribuições da Amazon estão usando um certificado SSL personalizado e estão configuradas para usar o SNI para atender solicitações HTTPS. A regra será NON_COMPLIANT se um certificado SSL personalizado estiver associado, mas o método de suporte SSL for um endereço IP dedicado.

Identificador: CLOUDFRONT_SNI_ENABLED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-traffic-to-origin-encrypted

Verifica se CloudFront as distribuições da Amazon estão criptografando o tráfego para origens personalizadas. A regra é NON_COMPLIANT se 'OriginProtocolPolicy' for 'http-only' ou se 'Policy' for' match-viewer 'e' OriginProtocol Policy' for 'allow-all'. ViewerProtocol

Identificador: CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudfront-viewer-policy-https

Verifica se suas CloudFront distribuições da Amazon usam HTTPS (diretamente ou por meio de um redirecionamento). A regra é NON_COMPLIANT se o valor de ViewerProtocolPolicy for definido como 'allow-all' para o ou para o. DefaultCacheBehavior CacheBehaviors

Identifier (Identificador): CLOUDFRONT_VIEWER_POLICY_HTTPS

Tipos de recursos: AWS::CloudFront::Distribution

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

verificação de eventos de dados cloudtrail-all-read-s3-

Verifica se uma trilha AWS CloudTrail multirregional está ativada e registra todos os eventos de dados lidos do S3 para seus buckets. A regra é NON_COMPLIANT se nenhuma trilha multirregional registrar todos os tipos de eventos de dados do S3 lidos para todos os buckets atuais e futuros do S3.

Identificador: CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudtrail-all-write-s3-data-event-check

Verifica se uma trilha AWS CloudTrail multirregional está ativada e registra todos os eventos de dados de gravação do S3 para seus buckets. A regra é NON_COMPLIANT se nenhum registro de trilha multirregional gravar todos os tipos de eventos de dados do S3 para todos os buckets atuais e futuros do S3.

Identificador: CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

registro de acesso ao bucket do cloudtrail-s3-

Verifica se as configurações do bucket do S3 para seus AWS CloudTrail registros têm o registro de acesso ao servidor Amazon S3 ativado. A regra é NON_COMPLIANT se pelo menos um bucket do S3 para uma CloudTrail trilha não tiver o registro de acesso ao servidor do S3 ativado.

Identificador: CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

Tipos de recursos: AWS::CloudTrail::Trail

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

cloudtrail-s3-bucket-public-access proibido

Verifica se as configurações do bucket do S3 para seus AWS CloudTrail registros bloqueiam o acesso público. A regra é NON_COMPLIANT se pelo menos um bucket do S3 para uma CloudTrail trilha estiver acessível ao público.

Identificador: CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROBIBID

Tipos de recursos: AWS::CloudTrail::Trail

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudtrail-s3-dataevents-enabled

Verifica se pelo menos uma AWS CloudTrail trilha está registrando eventos de dados do Amazon Simple Storage Service (Amazon S3) para todos os buckets do S3. A regra será NON_COMPLIANT se houver trilhas ou se nenhuma trilha registrar eventos de dados do S3.

Identifier (Identificador): CLOUDTRAIL_S3_DATAEVENTS_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

S3 BucketNames (opcional), Tipo: string

> Lista separada por vírgulas de nomes de bucket do S3 para os quais o registro em log de eventos de dados deve ser habilitado. Verificações de comportamento padrão para todos os buckets do S3.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudtrail-security-trail-enabled

Verifica se há pelo menos uma AWS CloudTrail trilha definida com as melhores práticas de segurança. Essa regra será COMPLIANT se houver pelo menos uma trilha que atenda a todos os seguintes itens:

- eventos de serviços globais de registros
- é uma trilha multirregional
- tem a validação do arquivo de log habilitada

- criptografado com uma chave do KMS
- registra eventos para leituras e gravações
- eventos de gerenciamento de registros
- não exclui nenhum evento de gerenciamento

Essa regra será NON_COMPLIANT se nenhuma trilha atender a todos os critérios mencionados acima.

Identificador: CLOUDTRAIL_SECURITY_TRAIL_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

cloudwatch-alarm-action-check

Verifica se CloudWatch os alarmes têm uma ação configurada para o estado ALARM, INSUFFICIENT_DATA ou OK. Como opção, verifica se alguma ação corresponde a um ARN nomeado. A regra será NON_COMPLIANT se não houver nenhuma ação especificada para o alarme ou parâmetro opcional.

Identifier (Identificador): CLOUDWATCH_ALARM_ACTION_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

alarme ActionRequired, Tipo: string, Padrão: True

Os alarmes têm pelo menos uma ação.

insuficiente DataAction Obrigatório, Tipo: string, Padrão: True

Os alarmes têm pelo menos uma ação quando o alerta muda para o estado INSUFFICIENT_DATA de qualquer outro estado.

ok ActionRequired, Tipo: string, Padrão: False

Os alarmes têm pelo menos uma ação quando o alerta muda para um estado OK de qualquer outro estado.

ação1 (opcional), Tipo: string

A ação para executar, especificada como um ARN.

ação2 (opcional), Tipo: string

A ação para executar, especificada como um ARN.

ação3 (opcional), Tipo: string

A ação para executar, especificada como um ARN.

ação4 (opcional), Tipo: string

A ação para executar, especificada como um ARN.

ação5 (opcional), Tipo: string

A ação para executar, especificada como um ARN.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudwatch-alarm-action-enabled-check

Verifica se as ações de CloudWatch alarmes da Amazon estão ativadas. A regra é NON_COMPLIANT se as ações de CloudWatch alarme não estiverem no estado habilitado.

Identificador: CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudwatch-alarm-resource-check

Verifica se um tipo de recurso tem um CloudWatch alarme para a métrica nomeada. Para o tipo de recurso, você pode especificar volumes EBS, instâncias EC2, clusters do Amazon RDS ou buckets do S3. A regra é COMPATÍVEL se a métrica nomeada tiver um ID de recurso e um CloudWatch alarme.

Identifier: CLOUDWATCH_ALARM_RESOURCE_CHECK

Tipos de recursos: AWS::EC2::Instance, AWS::RDS::DBCluster, AWS::S3::Bucket, AWS::EC2::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceType, Tipo: string

AWS tipo de recurso. O valor pode ser um dos seguintes: AWS::EC2::Volume, AWS::EC2::Instance, AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, Tipo: string

O nome da métrica associada ao alarme (por exemplo, "CPUUtilization" para instâncias do EC2).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudwatch-alarm-settings-check

Verifica se CloudWatch os alarmes com o nome da métrica fornecida têm as configurações especificadas.

Identifier (Identificador): CLOUDWATCH_ALARM_SETTINGS_CHECK

Tipos de recursos: AWS::CloudWatch::Alarm

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

metricName, Tipo: string

O nome da métrica associado ao alarme.

threshold (opcional), Tipo: int

O valor em relação ao qual a estatística especificada é comparada.

evaluationPeriods (opcional), Tipo: int

O número de períodos com os quais os dados são comparados ao limite especificado.

period (opcional), Tipo: int, Padrão: 300

O período, em segundos, durante o qual a estatística especificada é aplicada.

comparisonOperator (opcional), Tipo: string

A operação para comparar a estatística e o limite especificados (por exemplo, 'GreaterThanLimite').

statistic (opcional), Tipo: string

A estatística para a métrica associada ao alarme (por exemplo, "Average" ou "Sum").

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudwatch-log-group-encrypted

Verifica se os grupos de CloudWatch log da Amazon estão criptografados com alguma chave AWS KMS ou um ID de chave AWS KMS especificado. A regra é NON_COMPLIANT se um grupo de CloudWatch registros não estiver criptografado com uma chave KMS ou for criptografado com uma chave KMS não fornecida no parâmetro da regra.

Identifier (Identificador): CLOUDWATCH_LOG_GROUP_ENCRYPTED

Tipos de recursos: AWS::Logs::LogGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

KmsKeyId (Opcional), Tipo: string

> Nome de recurso da Amazon (ARN) do ID da chave do KMS usada para criptografar o grupo de logs.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloud-trail-cloud-watch-logs-enabled

Verifica se as AWS CloudTrail trilhas estão configuradas para enviar registros para CloudWatch registros. A trilha não é compatível se a CloudWatchLogsLogGroupArn propriedade da trilha estiver vazia.

Identifier (Identificador): CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

esperado DeliveryWindowAge (opcional), Tipo: int

Idade máxima em horas da entrega mais recente aos CloudWatch registros que satisfaça a conformidade.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloudtrail-enabled

> **Important**
>
> Para essa regra, o identificador da regra (CLOUD_TRAIL_ENABLED) e o nome da regra (cloudtrail-enabled) são diferentes.

Verifica se uma AWS CloudTrail trilha está ativada em sua AWS conta. A regra será NON_COMPLIANT, se uma trilha não estivar habilitada. Opcionalmente, a regra verifica um bucket do S3 específico, um tópico do Amazon Simple Notification Service (Amazon SNS) e um grupo de registros. CloudWatch

Identifier (Identificador): CLOUD_TRAIL_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

s3 BucketName (opcional), Tipo: string

Nome do bucket do S3 para o CloudTrail qual entregar os arquivos de log.

snsTopicArn (Opcional), Tipo: string

ARN do tópico do SNS CloudTrail para uso em notificações.

nuvem WatchLogsLogGroupArn (opcional), Tipo: string

CloudWatch ARN do grupo de registros para o CloudTrail qual enviar dados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloud-trail-encryption-enabled

Verifica se AWS CloudTrail está configurado para usar a criptografia de criptografia do lado do servidor AWS Key Management Service (SSE AWS KMS) (). A regra é COMPATÍVEL se KmsKeyId for definida.

Identifier (Identificador): CLOUD_TRAIL_ENCRYPTION_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cloud-trail-log-file-validation-enabled

Verifica se AWS CloudTrail cria um arquivo de resumo assinado com registros. AWS recomenda que a validação do arquivo seja ativada em todas as trilhas. A regra será NON_COMPLIANT se a validação não estiver habilitada.

Identifier (Identificador): CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

Tipos de recursos: AWS::CloudTrail::Trail

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cmk-backing-key-rotation-enabled

Verifica se a rotação automática de chaves está ativada para cada chave e corresponde ao ID da chave AWS KMS criada pelo cliente. A regra é NON_COMPLIANT se a função de gravador AWS Config de um recurso não tiver a permissão kms:. DescribeKey

> **Note**
>
> Alternância de chave automática não é compatível com chaves do KMS assimétricas, chaves do KMS de HMAC, chaves do KMS com material de chave importado ou chaves do KMS em armazenamentos de chave personalizados.

Identifier (Identificador): CMK_BACKING_KEY_ROTATION_ENABLED

Tipos de recursos: AWS::KMS::Key

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-artifact-encryption

Verifica se um AWS CodeBuild projeto tem criptografia habilitada para todos os seus artefatos. A regra será NON_COMPLIANT se 'encryptionDisabled' for definido como 'true' para qualquer configuração de artefato primário ou secundário (se houver).

Identificador: CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-environment-privileged-check

Verifica se um ambiente de AWS CodeBuild projeto tem o modo privilegiado ativado. A regra é NON_COMPLIANT para um CodeBuild projeto se 'PrivilegedMode' estiver definido como 'true'.

Identificador: CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

exemptedProjects (opcional), Tipo: Csv

Lista separada por vírgula de nomes de CodeBuild projetos que podem ter 'PrivilegedMode' com valor 'true'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-envvar-awscred-check

Verifica se o projeto contém as variáveis de ambiente _ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY. AWS A regra será NON_COMPLIANT quando as variáveis de ambiente do projeto contiverem credenciais em texto simples.

Identificador: CODEBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-logging-enabled

Verifica se um ambiente de AWS CodeBuild projeto tem pelo menos uma opção de log ativada. A regra será NON_COMPLIANT se o status de todas as configurações de log atuais estiver definido como 'DISABLED'.

Identificador: CODEBUILD_PROJECT_LOGGING_ENABLED

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

s3 BucketNames (opcional), Tipo: string

Lista separada por vírgulas dos nomes de bucket do Amazon S3 para os quais os logs devem ser enviados, se os logs do S3 estiverem configurados.

nuvem WatchGroupNames (opcional), Tipo: string

Lista separada por vírgula dos nomes dos grupos de CloudWatch registros da Amazon para os quais os registros devem ser enviados se CloudWatch os registros estiverem configurados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-s3-logs-encrypted

Verifica se um AWS CodeBuild projeto configurado com o Amazon S3 Logs tem criptografia habilitada para seus registros. A regra é NON_COMPLIANT se 'EncryptionDisabled' estiver definido como 'true' em um S3 de um projeto. LogsConfig CodeBuild

Identificador: CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

exemptedProjects (opcional), Tipo: Csv

Lista separada por vírgula de nomes de CodeBuild projetos que podem gerar registros não criptografados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codebuild-project-source-repo-url-check

Verifica se o URL do repositório de origem do Bitbucket contém credenciais de login ou não. A regra será NON_COMPLIANT se o URL contiver alguma informação de login e COMPLIANT se não tiver.

Identifier (Identificador): CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Tipos de recursos: AWS::CodeBuild::Project

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codedeploy-auto-rollback-monitor-enabled

Verifica se o grupo de implantação está configurado com reversão automática de implantação e monitoramento de implantação com alarmes anexados. A regra é NON_COMPLIANT se AutoRollbackConfiguration não AlarmConfiguration tiver sido configurada ou não estiver habilitada.

Identificador: CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codedeploy-ec2-minimum-healthy-hosts-configured

Verifica se o grupo de implantação da EC2/On-Premises Compute Platform está configurado com uma porcentagem mínima da frota de hosts íntegros ou uma contagem de hosts maior ou igual ao limite de entrada. A regra será NON_COMPLIANT se alguma delas estiver abaixo do limite.

Identificador: CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mínimo HealthyHostsFleetPercent (opcional), Tipo: int, Padrão: 66

Porcentagem mínima de frota de hosts íntegros durante a implantação. O valor padrão é definido como 66%.

mínimo HealthyHostsHostCount (opcional), Tipo: int, Padrão: 1

Número mínimo de hosts íntegros na frota durante a implantação. O valor padrão é definido como 1.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codedeploy-lambda-allatonce-traffic-shift-disabled

Verifica se o grupo de implantação da Lambda Compute Platform não está usando a configuração de implantação padrão. A regra é NON_COMPLIANT se o grupo de implantação estiver usando a configuração de implantação 'Default. CodeDeploy LambdaAllAtOnce'.

Identificador: CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

Tipos de recursos: AWS::CodeDeploy::DeploymentGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codepipeline-deployment-count-check

Verifica se o primeiro estágio de implantação do AWS CodePipeline realiza mais de uma implantação. Verifica opcionalmente se cada um dos estágios subsequentes restantes implantam mais do que o número especificado de implantações (`deploymentLimit`).

Identifier (Identificador): CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

Tipos de recursos: AWS::CodePipeline::Pipeline

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível nas regiões Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (N. da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central)

Parâmetros:

deploymentLimit (opcional), Tipo: int

O número máximo de implantações que cada estágio pode executar.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

codepipeline-region-fanout-check

Verifica se cada estágio do é AWS CodePipeline implantado em mais de N vezes o número de regiões implantadas em todos os estágios combinados anteriores, onde N é o número de expansão da região. AWS CodePipeline O primeiro estágio de implantação pode ser implantado no máximo em uma região e o segundo estágio pode ser implantado no número máximo especificado no `regionFanoutFactor`. Se você não fornecer um `regionFanoutFactor`, por padrão, o valor será três. Por exemplo: se o primeiro estágio de implantação for implantado em uma região e o segundo estágio for implantado em três regiões, o terceiro estágio poderá ser implantado em 12 regiões, ou seja, a soma dos estágios anteriores multiplicada pelo número "fanout" de regiões (três). A regra será NON_COMPLIANT se a implantação estiver em mais de uma região no primeiro estágio ou em três regiões no segundo estágio ou em 12 regiões no terceiro estágio.

Identifier (Identificador): CODEPIPELINE_REGION_FANOUT_CHECK

Tipos de recursos: AWS::CodePipeline::Pipeline

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível nas regiões Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (N. da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central)

Parâmetros:

regionFanoutFactor (Opcional), Tipo: int, Padrão: 3

> O número de regiões em AWS CodePipeline que foi implantado em todos os estágios anteriores é o número aceitável de regiões nas quais qualquer estágio pode ser implantado.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

custom-eventbus-policy-attached

Verifica se os ônibus de eventos EventBridge personalizados da Amazon têm uma política baseada em recursos anexada. A regra será NON_COMPLIANT se uma política de barramento de eventos personalizada não tiver uma política com base em recursos anexada.

Identificador: CUSTOM_EVENTBUS_POLICY_ATTACHED

Tipos de recursos: AWS::Events::EventBus

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

custom-schema-registry-policy-attached

Verifica se os registros personalizados do EventBridge esquema da Amazon têm uma política de recursos anexada. A regra é NON_COMPLIANT para registros de esquemas personalizados sem uma política de recursos anexada.

Identificador: CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

Tipos de recursos: AWS::EventSchemas::Registry

Trigger type (Tipo de trigger): periódico

Região da AWS: Disponível somente na Europa (Estocolmo), Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Ásia-Pacífico (Hong Kong), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Ásia-Pacífico (Cingapura)), região Ásia-Pacífico (Sydney), Canadá (Central)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

cw-loggroup-retention-period-check

Verifica se um período CloudWatch LogGroup de retenção da Amazon está definido para mais de 365 dias ou então um período de retenção especificado. A regra é NON_COMPLIANT se o período de retenção for menor que`MinRetentionTime`, se especificado, ou então 365 dias.

> **Note**
>
> Se a configuração de retenção for “Nunca expirar” para um grupo de logs, a regra será marcada como COMPLIANT.

Identificador: CW_LOGGROUP_RETENTION_PERIOD_CHECK

Tipos de recursos: AWS::Logs::LogGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

LogGroupNames (Opcional), Tipo: Csv

Uma lista separada por vírgulas de nomes de grupos de logs para verificar o período de retenção.

MinRetentionTime (Opcional), Tipo: int

Especifique o tempo de retenção. Os valores válidos são: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827 e 3653. O período de retenção padrão é 365 dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dax-encryption-enabled

Verifica se os clusters do Amazon DynamoDB Accelerator (DAX) estão criptografados. A regra será NON_COMPLIANT se o cluster do DAX não estiver criptografado.

Identificador: DAX_ENCRYPTION_ENABLED

Tipos de recursos: AWS::DAX::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível em Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (N. da Virgínia), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

criptografia de endpoint dax-tls-

Verifica se o seu cluster do Amazon DynamoDB Accelerator (DAX) foi configurado como TLS. ClusterEndpointEncryptionType A regra é NON_COMPLIANT se um cluster DAX não for criptografado pela segurança da camada de transporte (TLS).

Identificador: DAX_TLS_ENDPOINT_ENCRYPTION

Tipos de recursos: AWS::DAX::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível em Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (N. da Virgínia), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

db-instance-backup-enabled

Verifica se as instâncias de banco de dados do RDS têm os backups habilitados. Opcionalmente, a regra verifica o período de retenção de backup e a janela de backup.

Identifier (Identificador): DB_INSTANCE_BACKUP_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

backupRetentionPeriod (Opcional), Tipo: int

O período de retenção dos backups.

backupRetentionMinimum (Opcional), Tipo: int

O período mínimo de retenção dos backups.

preferredBackupWindow (Opcional), Tipo: string

Intervalo de tempo em que os backups são criados.

checkReadReplicas (Opcional), Tipo: booliano

Verifica se as instâncias de banco de dados do RDS têm backups habilitados para réplicas de leitura.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

desired-instance-tenancy

Verifica as instâncias do EC2 em busca de um valor de “locação”. Também verifica se as IDs de AMI estão especificadas para serem iniciadas a partir dessas AMIs ou se as IDs de host são iniciadas nesses hosts dedicados. A regra será COMPLIANT se a instância corresponder a um host e a uma AMI, se especificada, em uma lista.

Identifier (Identificador): DESIRED_INSTANCE_TENANCY

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

locação, Tipo: string

A locação desejada das instâncias. Os valores válidos são DEDICATED, HOST e DEFAULT.

imageId (opcional), Tipo: Csv

A regra avalia instâncias executadas apenas a partir dos AMIs com os IDs especificados. Separe com vírgulas os vários IDs de AMI.

hostId (opcional), Tipo: Csv

Os IDs de host dedicado do EC2 no qual as instâncias devem ser executadas. Separe com vírgulas os vários IDs de host.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

desired-instance-type

Verifica se suas instâncias EC2 são de um tipo de instância específico. A regra será NON_COMPLIANT se uma instância do EC2 não for especificada na lista de parâmetros. Para obter uma lista dos tipos de instância EC2 com suporte, consulte tipos de instância no Guia do usuário do EC2 para instâncias do Linux.

Identifier (Identificador): DESIRED_INSTANCE_TYPE

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

instanceType, Tipo: Csv

Lista separada por vírgulas dos tipos de instâncias EC2 (por exemplo, "t2.small, m4.large, i2.xlarge").

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-auto-minor-version-upgrade-check

Verifica se uma instância de replicação do AWS Database Migration Service (AWS DMS) tem atualizações automáticas de versões secundárias habilitadas. A regra é NON_COMPLIANT se uma instância de replicação do AWS DMS não estiver configurada com atualizações automáticas de versões secundárias.

Identificador: DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipos de recursos: AWS::DMS::ReplicationInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-endpoint-ssl-configured

Verifica se os endpoints do AWS Database Migration Service (AWS DMS) estão configurados com uma conexão SSL. A regra é NON_COMPLIANT se o AWS DMS não tiver uma conexão SSL configurada.

Identificador: DMS_ENDPOINT_SSL_CONFIGURED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para autenticação dms-mongo-db

Verifica se os endpoints do AWS Database Migration Service (AWS DMS) para armazenamentos de MongoDb dados estão habilitados para autenticação baseada em senha e controle de acesso. A regra é NON_COMPLIANT se a autenticação baseada em senha e o controle de acesso não estiverem habilitados.

Identificador: DMS_MONGO_DB_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-neptune-iam com autorização habilitada

Verifica se um endpoint do AWS Database Migration Service (AWS DMS) para bancos de dados Amazon Neptune está configurado com autorização do IAM. A regra é NON_COMPLIANT se um AWS endpoint do DMS em que Neptune é o destino tiver sido definido como falso. IamAuthEnabled

Identificador: DMS_NEPTUNE_IAM_AUTHORIZATION_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para dms-redis-tls

Verifica se os endpoints do AWS Database Migration Service (AWS DMS) para armazenamentos de dados do Redis estão habilitados para criptografia TLS/SSL dos dados comunicados com outros endpoints. A regra é NON_COMPLIANT se a criptografia TLS/SSL não estiver habilitada.

Identificador: DMS_REDIS_TLS_ENABLED

Tipos de recursos: AWS::DMS::Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-replication-not-public

Verifica se as instâncias de replicação do AWS Database Migration Service (AWS DMS) são públicas. A regra será NON_COMPLIANT se o PubliclyAccessible campo for definido como verdadeiro.

Identifier (Identificador): DMS_REPLICATION_NOT_PUBLIC

Tipos de recursos: AWS::DMS::ReplicationInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-replication-task-sourcedb-logging

Verifica se o registro está habilitado com um nível de severidade válido para tarefas de replicação do AWS DMS de um banco de dados de origem. A regra será NON_COMPLIANT se o registro em log não estiver habilitado ou se os logs de tarefas de replicação do DMS de um banco de dados de origem tiverem um nível de severidade inválido.

Identificador: DMS_REPLICATION_TASK_SOURCEDB_LOGGING

Tipos de recursos: AWS::DMS::ReplicationTask

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dms-replication-task-targetdb-logging

Verifica se o registro está habilitado com um nível de severidade válido para eventos de tarefas de replicação do AWS DMS de um banco de dados de destino. A regra será NON_COMPLIANT se o registro em log não estiver habilitado ou se o registro em log de tarefas de replicação de um banco de dados de destino tiver um nível de severidade inválido.

Identificador: DMS_REPLICATION_TASK_TARGETDB_LOGGING

Tipos de recursos: AWS::DMS::ReplicationTask

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

docdb-cluster-audit-logging-enabled

Verifica se um cluster de instância do Amazon DocumentDB (com compatibilidade com o MongoDB) tem a exportação de CloudWatch log habilitada para registros de auditoria. A regra é NON_COMPLIANT se um cluster de instância do Amazon DocumentDB não tiver a exportação de CloudWatch log habilitada para registros de auditoria.

Identificador: DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região da Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central), China (Ningxia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

docdb-cluster-backup-retention-check

Verifica se o período de retenção de um cluster de banco de dados de documentos da Amazon está definido para um número específico de dias. A regra será NON_COMPLIANT se o período de retenção for menor que o valor especificado pelo parâmetro.

Identificador: DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região da Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central), China (Ningxia)

Parâmetros:

mínimo BackupRetentionPeriod (opcional), Tipo: int

Os backups mínimos de dias devem ser mantidos. Valores válidos de 1 a 35, o valor padrão é 7. Essa regra é NON_COMPLIANT se o valor for maior que 'backup'. RetentionPeriod

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

docdb-cluster-deletion-protection-enabled

Verifica se um cluster do Amazon DocumentDB (compatível com MongoDB) tem proteção de exclusão habilitada. A regra será NON_COMPLIANT se um cluster Amazon DocumentDB tiver o campo deletionProtection definido como falso.

Identificador: DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região da Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central), China (Ningxia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

docdb-cluster-encrypted

Verifica se a criptografia de armazenamento está habilitada para seus clusters do Amazon DocumentDB (compatível com MongoDB). A regra será NON_COMPLIANT se a criptografia de armazenamento não estiver habilitada.

Identificador: DOCDB_CLUSTER_ENCRYPTED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região da Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central), China (Ningxia)

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

> Uma lista separada por vírgulas de ARNs de chaves KMS para comparar com a KmsKey ID do cluster criptografado.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

docdb-cluster-snapshot-public-prohibited

Verifica se os snapshots manuais do cluster do Amazon DocumentDB são públicos. A regra será NON_COMPLIANT se qualquer snapshot manual do cluster do Amazon DocumentDB for público.

Identificador: DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Tipos de recursos: AWS: :RDS: :DB ClusterSnapshot

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (N. da

Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney) Canadá (Central)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

dynamodb-autoscaling-enabled

Verifica se as tabelas do Amazon DynamoDB ou os índices secundários globais podem processar a capacidade de leitura/gravação usando o modo sob demanda ou o modo provisionado com o ajuste de escala automático habilitado. A regra será NON_COMPLIANT se qualquer um dos modos for usado sem o ajuste de escala automático habilitado

Identifier (Identificador): DYNAMODB_AUTOSCALING_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

min ProvisionedReadCapacity (opcional), Tipo: int

O número mínimo de unidades que devem ser provisionadas com capacidade de leitura no grupo do Auto Scaling.

máximo ProvisionedReadCapacity (opcional), Tipo: int

O número máximo de unidades que devem ser provisionadas com capacidade de leitura no grupo do Auto Scaling.

targetReadUtilization (Opcional), Tipo: double

A porcentagem de utilização pretendida para a capacidade de leitura. A utilização prevista é expressa em termos da proporção de capacidade consumida e capacidade provisionada.

min ProvisionedWriteCapacity (opcional), Tipo: int

O número mínimo de unidades que devem ser provisionadas com capacidade de gravação no grupo do Auto Scaling.

máximo ProvisionedWriteCapacity (opcional), Tipo: int

O número máximo de unidades que devem ser provisionadas com capacidade de gravação no grupo do Auto Scaling.

targetWriteUtilization (Opcional), Tipo: double

A porcentagem de utilização pretendida para a capacidade de gravação. A utilização prevista é expressa em termos da proporção de capacidade consumida e capacidade provisionada.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-in-backup-plan

Verifica se a tabela do Amazon DynamoDB está presente nos AWS Planos de Backup. A regra não é compatível se as tabelas do Amazon DynamoDB não estiverem presentes em nenhum plano de Backup. AWS

Identificador: DYNAMODB_IN_BACKUP_PLAN

Tipos de recursos: AWS::DynamoDB::Table

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para as tabelas do Amazon DynamoDB dentro do período especificado. A regra será NON_COMPLIANT se a tabela do DynamoDB não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::DynamoDB::Table

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags das tabelas do DynamoDB para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

Nome da tabela do DynamoDB para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

dynamodb-meets-restore-time-target

Confere se o tempo de restauração das tabelas do Amazon DynamoDB atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes uma tabela do DynamoDB for maior que minutos. maxRestoreTime

Identificador: DYNAMODB_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::DynamoDB::Table

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags das tabelas do DynamoDB para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

Nome da tabela do DynamoDB para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-pitr-enabled

Verifica se a point-in-time recuperação (PITR) está habilitada para tabelas do Amazon DynamoDB. A regra será NON_COMPLIANT se PITR não estiver habilitada para tabelas do DynamoDB.

Identificador: DYNAMODB_PITR_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-resources-protected-by-backup-plan

Verifica se as tabelas do Amazon DynamoDB estão protegidas por um plano de backup. A regra será NON_COMPLIANT se a tabela do DynamoDB não estiver coberta por um plano de backup.

Identificador: DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::DynamoDB::Table

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para tabelas do DynamoDB para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

Nome da tabela do DynamoDB para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-table-deletion-protection-enabled

Verifica se uma tabela do Amazon DynamoDB tem a proteção de exclusão definida como habilitada. A regra será NON_COMPLIANT se a tabela tiver a proteção contra exclusão definida como desabilitada.

Identificador: DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-table-encrypted-kms

Verifica se a tabela do Amazon DynamoDB está criptografada AWS com o Key Management Service (KMS). A regra é NON_COMPLIANT se a tabela do Amazon DynamoDB não estiver criptografada com o KMS. AWS A regra também é NON_COMPLIANT se a chave AWS KMS criptografada não estiver presente no parâmetro de entrada. `kmsKeyArns`

Identificador: DYNAMODB_TABLE_ENCRYPTED_KMS

Tipos de recursos: AWS::DynamoDB::Table

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

> Lista separada por vírgula de ARNs de chave AWS KMS permitida para criptografar tabelas do Amazon DynamoDB.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-table-encryption-enabled

Verifica se as tabelas do Amazon DynamoDB são criptografadas e verifica seu status. A regra será COMPLIANT se o status for habilitado ou em habilitação.

Identifier (Identificador): DYNAMODB_TABLE_ENCRYPTION_ENABLED

Tipos de recursos: AWS::DynamoDB::Table

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

dynamodb-throughput-limit-check

Verifica se o throughput provisionado do DynamoDB está se aproximando do limite máximo para a sua conta. Por padrão, a regra verifica se o throughput provisionado excede a marca de 80% dos limites de sua conta.

Identifier (Identificador): DYNAMODB_THROUGHPUT_LIMIT_CHECK

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Conta RCU (opcional) ThresholdPercentage , Tipo: int, Padrão: 80

> Porcentagem de unidades de capacidade de leitura provisionada para a sua conta. Quando esse valor é atingido, a regra é marcada como não compatível.

Conta WCU (opcional) ThresholdPercentage , Tipo: int, Padrão: 80

> Porcentagem de unidades de capacidade de gravação provisionada para a sua conta. Quando esse valor é atingido, a regra é marcada como não compatível.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ebs-in-backup-plan

Verifique se os volumes do Amazon Elastic Block Store (Amazon EBS) foram adicionados aos planos de backup do Backup. AWS A regra será NON_COMPLIANT se os volumes do Amazon EBS não estiverem incluídos nos planos de backup.

Identificador: EBS_IN_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ebs-last-backup-recovery-point-created

Verifica se foi criado um ponto de recuperação para o Amazon Elastic Block Store (Amazon EBS). A regra será NON_COMPLIANT se o volume do Amazon EBS não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::EC2::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos volumes do Amazon EBS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do volume do Amazon EBS para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ebs-meets-restore-time-target

Confere se o tempo de restauração dos volumes do Amazon Elastic Block Store (Amazon EBS) atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes um volume do Amazon EBS for maior que minutos. maxRestoreTime

Identificador: EBS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::EC2::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags para volumes do Amazon EBS para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID do volume do Amazon EBS para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ebs-optimized-instance

Verifica se a otimização do Amazon EBS está habilitada para suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que podem ser otimizadas para o Amazon EBS. A regra será

NON_COMPLIANT se a otimização do EBS não estiver habilitada para uma instância do Amazon EC2 que pode ser otimizada para o EBS.

> **Note**
>
> As instâncias do EC2 que são otimizadas para EBS por padrão sempre resultam em avaliações de regra que retornam `COMPLIANT`.

Identifier (Identificador): EBS_OPTIMIZED_INSTANCE

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ebs-resources-protected-by-backup-plan

Verifica se os volumes do Amazon Elastic Block Store (Amazon EBS) estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o volume do Amazon EBS não estiver coberto por um plano de backup.

Identificador: EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para volumes do Amazon EBS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do volume do Amazon EBS para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ebs-snapshot-public-restorable-check

Verifica se snapshots do Amazon Elastic Block Store (Amazon EBS) não são restauráveis publicamente. A regra é NON_COMPLIANT se um ou mais snapshots com RestorableByUserIds campo estiverem definidos como todos, ou seja, os snapshots do Amazon EBS forem públicos.

Identifier (Identificador): EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-client-vpn-connection-log-enabled

Verifica se AWS o endpoint do Client VPN tem o registro de conexão do cliente ativado. A regra é NON_COMPLIANT se for 'Configuração'. ConnectionLogOptions.Enabled' está definido como false.

Identificador: EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

Tipos de recursos: AWS::EC2::ClientVpn Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-client-vpn-not-authorize-all

Verifica se as regras de autorização AWS do Client VPN autorizam o acesso à conexão para todos os clientes. A regra é NON_COMPLIANT se 'AccessAll' estiver presente e definida como verdadeira.

Identificador: EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

Tipos de recursos: AWS::EC2::ClientVpn Endpoint

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-ebs-encryption-by-default

Verifica se a criptografia do Amazon Elastic Block Store (EBS) está habilitada por padrão. A regra será NON_COMPLIANT se a criptografia não estiver habilitada.

Identificador: EC2_EBS_ENCRYPTION_BY_DEFAULT

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-imdsv2-check

Verifica se a versão de metadados de sua instância do Amazon Elastic Compute Cloud (Amazon EC2) está configurada com o serviço de metadados de instância versão 2 (IMDSv2). A regra é NON_COMPLIANT se HttpTokens for definida como opcional.

Identificador: EC2_IMDSV2_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-instance-detailed-monitoring-enabled

Verifica se o monitoramento detalhado está habilitado para instâncias do EC2. A regra será NON_COMPLIANT se o monitoramento detalhado não estiver habilitado.

Identifier (Identificador): EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-instance-managed-by-systems-manager

> **Important**
>
> Para essa regra, o identificador da regra (EC2_INSTANCE_MANAGED_BY_SSM) e o nome da regra (ec2-instance-managed-by-systems-manager) são diferentes.

Verifica se suas instâncias do Amazon EC2 são gerenciadas pelo AWS Systems Manager Agente (SSM Agent). A regra é NON_COMPLIANT se uma instância do EC2 estiver em execução e o SSM Agent estiver parado, ou se uma instância do EC2 estiver em execução e o SSM Agent for encerrado.

> **Note**
>
> A regra não retornará NON_COMPLIANT se uma instância do EC2 for interrompida e o agente SSM estiver em execução.

Identificador: EC2_INSTANCE_MANAGED_BY_SSM

Tipos de recursos: AWS::EC2::Instance, AWS::SSM::ManagedInstance Inventário

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ec2-instance-multiple-eni-check

Verifica se o Amazon Elastic Compute Cloud (Amazon EC2) usa várias interfaces de rede elástica (ENIs) ou Elastic Fabric Adapters (EFAs). A regra é NON_COMPLIANT, uma instância do Amazon EC2 usa várias interfaces de rede.

Identificador: EC2_INSTANCE_MULTIPLE_ENI_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

NetworkInterfaceIds (Opcional), Tipo: Csv

Lista separada por vírgulas de IDs da instância de rede

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-instance-no-public-ip

Verifica se as instâncias do EC2 possuem uma associação de IP público. A regra será NON_COMPLIANT se o campo publicIp estiver presente no item de configuração da instância do EC2. Esta regra se aplica somente a IPv4.

Contexto: endereços IP públicos podem tornar as instâncias do EC2 diretamente acessíveis pela internet, o que nem sempre é desejável do ponto de vista de segurança ou conformidade:

- Segurança: em muitos casos, talvez você não queira que suas instâncias do EC2 tenham endereços IP públicos, a menos que precisem estar acessíveis ao público. Ter um endereço IP público pode expor sua instância do EC2 a possíveis riscos de segurança, como acesso não autorizado ou ataques.

- Conformidade: vários padrões de conformidade, como PCI, DSS ou HIPAA, têm requisitos específicos em relação à segmentação da rede e aos controles de acesso. Garantir que as instâncias do EC2 não tenham endereços IP públicos desnecessários pode ajudar a garantir a conformidade com esses requisitos.
- Gerenciamento de custos: endereços IP públicos podem incorrer em custos adicionais, especialmente se houver instâncias do EC2 continuamente associadas a eles. Ao identificar instâncias do EC2 com IPs públicos que não precisam delas, você pode provavelmente reduzir custos.

Identifier (Identificador): EC2_INSTANCE_NO_PUBLIC_IP

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-instance-profile-attached

Verifica se uma instância do EC2 tem um perfil AWS Identity and Access Management (IAM) anexado a ela. A regra será NON_COMPLIANT se nenhum perfil do IAM estiver vinculado à instância do EC2.

Identificador: EC2_INSTANCE_PROFILE_ATTACHED

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

IamInstanceProfileArnList (Opcional), Tipo: Csv

Lista separada por vírgulas de nomes dos recursos da Amazon (ARNs) do perfil do IAM que podem ser anexados às instâncias do Amazon EC2.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para instâncias do Amazon Elastic Compute Cloud (Amazon EC2). A regra será NON_COMPLIANT se a instância do Amazon EC2 não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::EC2::Instance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags de instâncias do Amazon EC2 para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID da instância do Amazon EC2 para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-launch-template-public-ip-disabled

Verifica se os modelos de execução do Amazon EC2 estão configurados para atribuir endereços IP públicos às interfaces de rede. A regra é NON_COMPLIANT se a versão padrão de um modelo de inicialização do EC2 tiver pelo menos 1 interface de rede com '' definido como AssociatePublic IpAddress 'verdadeiro'.

Identificador: EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::EC2::LaunchTemplate

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

exemptedLaunchTemplates (Opcional), Tipo: Csv

> Lista separada por vírgula de IDs de modelo de lançamento do EC2 isentos que podem ter interfaces de rede com o valor definido como 'verdadeiro'. AssociatePublicIpAddress

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-applications-blacklisted

Verifica se nenhuma das aplicações especificadas estão instaladas na instância. Há a opção de especificar a versão. As versões mais recentes não serão negadas. Opcionalmente, especifique a plataforma para aplicar a regra apenas para instâncias que estejam executando essa plataforma.

Identifier (Identificador): EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Tipos de recursos: AWS::SSM::ManagedInstance Inventário

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

applicationNames, Tipo: Csv

Uma lista separada por vírgulas de nomes de aplicações. Opcionalmente, especifique as versões anexadas com ":" (por exemplo, "Chrome:0.5.3, FireFox").

> **Note**
>
> Os nomes das aplicações precisam ter uma correspondência exata. Por exemplo, use **`firefox`** no Linux ou **`firefox-compat`** no Amazon Linux. Além disso, atualmente AWS Config não oferece suporte a curingas para o parâmetro ApplicationNames (por exemplo,). **`firefox*`**

platformType (opcional), Tipo: string

O tipo de plataforma (por exemplo, "Linux" ou "Windows").

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-applications-required

Verifica se todas as aplicações especificadas estão instaladas na instância. Opcionalmente, especifique a versão mínima aceitável. Você também pode especificar a plataforma para aplicar a regra somente às instâncias em execução na plataforma.

> **Note**
>
> Certifique-se de que o SSM Agent esteja sendo executado na instância do EC2 e que uma associação para coletar o inventário do software da aplicação seja criada. A regra retornará NOT_APPLICABLE se o SSM Agent não estiver instalado ou se uma associação ainda não tiver sido criada ou em estiver em execução.

Identifier (Identificador): EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Tipos de recursos: AWS::SSM::ManagedInstance Inventário

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

applicationNames, Tipo: Csv

Uma lista separada por vírgulas de nomes de aplicações. Opcionalmente, especifique as versões anexadas com ":" (por exemplo, "Chrome:0.5.3, FireFox").

> **Note**
>
> Os nomes das aplicações precisam ter uma correspondência exata. Por exemplo, use **`firefox`** no Linux ou **`firefox-compat`** no Amazon Linux. Além disso, atualmente AWS Config não oferece suporte a curingas para o parâmetro ApplicationNames (por exemplo,). **`firefox*`**

platformType (opcional), Tipo: string

O tipo de plataforma (por exemplo, "Linux" ou "Windows").

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-association-compliance-status-check

Verifica se o status da conformidade da associação do AWS Systems Manager é COMPATÍVEL ou NÃO COMPATÍVEL após a execução da associação na instância. A regra será compatível se o campo status for COMPATÍVEL. Para obter mais informações sobre associações, consulte What is an association?.

Identifier (Identificador): EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

Tipos de recursos: AWS::SSM::AssociationCompliance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-inventory-blacklisted

Verifica se as instâncias gerenciadas pelo Amazon EC2 Systems Manager estão configuradas para coletar os tipos de estoque na lista de restrições.

Identifier (Identificador): EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

Tipos de recursos: AWS::SSM::ManagedInstance Inventário

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

inventoryNames, Tipo: Csv

Lista separada por vírgula dos tipos de inventário do Systems Manager (por exemplo, ':Network AWS,: AWS'). WindowsUpdate

platformType (opcional), Tipo: string

Tipo de plataforma (por exemplo, “Linux”).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-patch-compliance-status-check

Verifica se o status de conformidade da conformidade do patch do AWS Systems Manager é COMPATÍVEL ou NÃO COMPATÍVEL após a instalação do patch na instância. A regra será compatível se o campo status for COMPATÍVEL.

Identifier (Identificador): EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

Tipos de recursos: AWS::SSM::PatchCompliance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-managedinstance-platform-check

Verifica se as instâncias gerenciadas do EC2 possuem as configurações desejadas.

Identifier (Identificador): EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Tipos de recursos: AWS::SSM::ManagedInstance Inventário

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

platformType, Tipo: string

Tipo de plataforma (por exemplo, “Linux”).

platformVersion (opcional), Tipo: string

A versão da plataforma (por exemplo, "2016.09").

agentVersion (opcional), Tipo: string

Versão do agente (por exemplo, '2.0.433.0').

platformName (opcional), Tipo: string

A versão da plataforma (por exemplo, "2016.09")

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-meets-restore-time-target

Confere se o tempo de restauração das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes uma instância do Amazon EC2 for maior que minutos. maxRestoreTime

Identificador: EC2_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::EC2::Instance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags de instâncias do Amazon EC2 para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID da instância do Amazon EC2 para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-no-amazon-key-pair

Verifica se as instâncias do Amazon Elastic Compute Cloud (EC2) foram iniciadas por pares de chaves do Amazon. A regra será NON_COMPLIANT se uma instância do EC2 em execução for iniciada com um par de chaves.

Identificador: EC2_NO_AMAZON_KEY_PAIR

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-paravirtual-instance-check

Verifica se o tipo de virtualização de uma instância do EC2 é paravirtual. Essa regra é NON_COMPLIANT para uma instância do EC2 se 'virtualizationType' estiver definido como 'paravirtual'.

Identificador: EC2_PARAVIRTUAL_INSTANCE_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível nas regiões da China (Pequim), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Tóquio),

Oeste dos EUA (Oregon), Oeste dos EUA (N. da Califórnia), Ásia-Pacífico (Singapura) e Ásia-Pacífico (Sydney).

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ec2-resources-protected-by-backup-plan

Verifica se instâncias do Amazon Elastic Compute Cloud (Amazon EC2) estão protegidas por um plano de backup. A regra será NON_COMPLIANT se a instância do Amazon EC2 não estiver coberta por um plano de backup.

> **Note**
>
> Essa regra é aplicável somente à execução de instâncias do Amazon EC2 e não às instâncias que estão desabilitadas.

Identificador: EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EC2::Instance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para instâncias do Amazon EC2 para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID da instância do Amazon EC2 para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-security-group-attached-to-eni

Verifica se grupos de segurança não padrão estão conectados às interfaces de rede elástica. A regra será NON_COMPLIANT se o grupo de segurança não estiver associado a uma interface de rede.

Identifier (Identificador): EC2_SECURITY_GROUP_ATTACHED_TO_ENI

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-security-group-attached-to-eni-periodic

Verifica se grupos de segurança não padrão estão conectados às interfaces de rede elásticas (ENIs). A regra será NON_COMPLIANT se o grupo de segurança não estiver associado a uma ENI. Grupos de segurança não pertencentes à conta de chamada são avaliados como NOT_APPLICABLE.

> **Note**
>
> Essa regra informa sobre o tipo de recurso `AWS::EC2::SecurityGroup`. No entanto, para que a regra seja executada com eficiência, é necessário habilitar a gravação do tipo de recurso `AWS::EC2::NetworkInterface`.

Identificador: EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

Tipos de recursos: AWS::EC2::SecurityGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-stopped-instance

Verifica se há instâncias do Amazon Elastic Compute Cloud (Amazon EC2) paradas por mais do que o número de dias permitido. A regra será NON_COMPLIANT se o estado da instância do Amazon

EC2 tiver sido interrompido por mais tempo do que o número de dias permitido, ou se o tempo não pode ser determinado.

Identifier (Identificador): EC2_STOPPED_INSTANCE

Tipos de recursos: AWS::EC2::Instance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

AllowedDays (Opcional), Tipo: int, Padrão: 30

O número de dias em que uma instância do Amazon EC2 pode ser interrompida antes da regra ser NON_COMPLIANT. O número padrão de dias é 30.

> **Note**
>
> O número de dias selecionados precisa ser menor que o período de retenção configurado, pois essa regra depende dos dados históricos coletados. Para obter mais informações sobre retenção de dados históricos, consulte Excluindo AWS Config dados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-token-hop-limit-check

Verifica se os metadados de uma instância do Amazon Elastic Compute Cloud (EC2) têm um limite de salto de token especificado que está abaixo do limite desejado. A regra é NON_COMPLIANT para uma instância se ela tiver um valor limite de salto acima do limite pretendido.

Identificador: EC2_TOKEN_HOP_LIMIT_CHECK

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

tokenHopLimit (Opcional), Tipo: int

O limite de salto de token desejado. Os valores válidos estão entre um e 64, ambos inclusive. O valor padrão será 1 se o parâmetro não for especificado.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-transit-gateway-auto-vpc-attach-disabled

Verifica se os gateways de trânsito do Amazon Elastic Compute Cloud (Amazon EC2) têm " ativado. AutoAccept SharedAttachments A regra é NON_COMPLIANT para um Transit Gateway se " estiver definido como AutoAccept SharedAttachments 'ativar'.

Identificador: EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

Tipos de recursos: AWS::EC2::TransitGateway

Tipo de trigger: alterações da configuração

Região da AWS: Disponível somente na Europa (Estocolmo), Europa (Paris), Leste dos EUA (Ohio), África (Cidade do Cabo), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Europa (Milão), Ásia-Pacífico (Tóquio), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Cingapura), Ásia Região Pacífico (Sydney), Canadá (Central)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-volume-inuse-check

Verifica se os volumes EBS estão anexados a instâncias do EC2. Opcionalmente, verifica se volumes EBS estão marcados para exclusão quando uma instância é encerrada.

A regra será COMPLIANT se um volume do EBS estiver vinculado a uma instância do EC2 em execução. Nesse caso, é COMPLIANT quando o volume do EBS está sendo usado ativamente por uma instância do EC2.

A regra será NON_COMPLIANT se um volume do EBS não estiver conectado a nenhuma instância do EC2 ou estiver vinculado a uma instância do EC2 interrompida ou encerrada. Nesse caso, é NON_COMPLIANT quando o volume do EBS não está sendo usado ativamente por uma instância do EC2.

Identifier (Identificador): EC2_VOLUME_INUSE_CHECK

Tipos de recursos: AWS::EC2::Volume

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

deleteOnTermination (Opcional), Tipo: booliano

> Os volumes EBS são marcados para exclusão quando uma instância é encerrada. Valores possíveis: verdadeiro ou falso (outros valores de entrada são marcados como NON_COMPLIANT). Se definido como `True`, a regra será NON_COMPLIANT se um volume encerrado do EBS não estiver marcado para exclusão.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecr-private-image-scanning-enabled

Verifica se um repositório privado do Amazon Elastic Container Registry (Amazon ECR) tem a verificação de imagens habilitada. A regra será NON_COMPLIANT se a frequência de verificação do repositório privado do Amazon ECR não estiver em verificação por push ou verificação contínua.

Para obter mais informações sobre a digitalização de imagens, consulte Digitalização de imagens no Guia do usuário do Amazon ECR.

Identificador: ECR_PRIVATE_IMAGE_SCANNING_ENABLED

Tipos de recursos: AWS::ECR::Repository

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecr-private-lifecycle-policy-configured

Verifica se um repositório privado do Amazon Elastic Container Registry (ECR) tem pelo menos uma política de ciclo de vida configurada. A regra será NON_COMPLIANT se nenhuma política de ciclo de vida estiver configurada para o repositório privado do ECR.

Identificador: ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

Tipos de recursos: AWS::ECR::Repository

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecr-private-tag-immutability-enabled

Verifica se um repositório privado do Amazon Elastic Container Registry (ECR) tem a imutabilidade de tags habilitada. Essa regra será NON_COMPLIANT se a imutabilidade da tag não estiver habilitada para o repositório ECR privado.

Identificador: ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

Tipos de recursos: AWS::ECR::Repository

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecs-awsvpc-networking-enabled

Verifica se o modo de rede do ECS ativo TaskDefinitions está definido como 'awsvpc'. Essa regra não é compatível se o ECS ativo não estiver definido como TaskDefinitions 'awsvpc'.

> **Note**
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: AWSVPC_NETWORKING ECS_ _ENABLED

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-containers-nonprivileged

Verifica se o parâmetro privilegiado na definição do contêiner do ECS TaskDefinitions está definido como 'verdadeiro'. A regra será NON_COMPLIANT se o parâmetro privilegiado for 'true'.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_CONTAINERS_NONPRIVILEGED

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-containers-readonly-access

Verifica se os contêineres do Amazon Elastic Container Service (Amazon ECS) têm acesso somente de leitura aos seus sistemas de arquivos raiz. A regra é NON_COMPLIANT se o

readonlyRootFilesystem parâmetro na definição do contêiner do ECS TaskDefinitions estiver definido como 'false'.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_CONTAINERS_READONLY_ACCESS

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecs-container-insights-enabled

Verifica se os clusters do Amazon Elastic Container Service têm insights de contêiner habilitados. A regra será NON_COMPLIANT se os insights do contêiner não estiverem habilitados.

Identificador: ECS_CONTAINER_INSIGHTS_ENABLED

Tipos de recursos: AWS::ECS::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-fargate-latest-platform-version

Verifica se os serviços do ECS Fargate estão configurados para a versão mais recente da plataforma. A regra é NON_COMPLIANT se, para PlatformVersion o Fargate, o tipo de lançamento não estiver definido como LATEST ou se latestLinuxVersion nenhum `latestWindowsVersion` deles for fornecido como parâmetro.

Identificador: ECS_FARGATE_LATEST_PLATFORM_VERSION

Tipos de recursos: AWS::ECS::Service

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

latestLinuxVersion (Opcional), Tipo: string

O Linux mais recente suportou PlatformVersion " no formato de versão semântica ()SemVer. O parâmetro pode ser necessário se o Fargate foi implantado e o 'PlatformVersion' foi explicitamente especificado ou CodeDeploy usado como " DeploymentController

latestWindowsVersion (Opcional), Tipo: string

O Windows mais recente suportou PlatformVersion " no formato de versão semântica ()SemVer. O parâmetro pode ser necessário se o Fargate foi implantado e o 'PlatformVersion' foi explicitamente especificado ou CodeDeploy usado como " DeploymentController

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-no-environment-secrets

Verifica se os segredos são passados como variáveis de ambiente do contêiner. A regra será NON_COMPLIANT se 1 ou mais chaves de variáveis de ambiente corresponderem a uma chave

listada no parâmetro '`secretKeys`' (excluindo variáveis ambientais de outros locais, como o Amazon S3).

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_NO_ENVIRONMENT_SECRETS

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

secretKeys, Tipo: Csv

Lista separada por vírgulas de nomes de chave a serem pesquisados nas variáveis de ambiente das definições de contêiner nas Definições de Tarefas. Os espaços extras serão removidos.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecs-task-definition-log-configuration

Verifica se o LogConfiguration está configurado nas definições de tarefas do ECS ativas. Essa regra é NON_COMPLIANT se um ECS ativo TaskDefinition não tiver o recurso LogConfiguration definido ou se o valor de LogConfiguration for nulo em pelo menos uma definição de contêiner.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_TASK_DEFINITION_LOG_CONFIGURATION

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-task-definition-memory-hard-limit

Verifica se as definições de tarefas do Amazon Elastic Container Service (ECS) têm um limite de memória definido para suas definições de contêiner. A regra será NON_COMPLIANT para uma definição de tarefa se o parâmetro 'memory' estiver ausente para uma definição de contêiner.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ecs-task-definition-nonroot-user

Verifica se o ECS TaskDefinitions especifica um usuário para que os contêineres do tipo de lançamento do Amazon Elastic Container Service (Amazon ECS) sejam executados no Amazon Elastic Container Service (Amazon ECS). A regra será NON_COMPLIANT se o parâmetro 'user' não estiver presente ou definido como 'root'.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_TASK_DEFINITION_NONROOT_USER

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecs-task-definition-pid-mode-check

Verifica se o ECS TaskDefinitions está configurado para compartilhar o namespace de processo de um host com seus contêineres do Amazon Elastic Container Service (Amazon ECS). A regra será NON_COMPLIANT se o parâmetro pidMode estiver definido como 'host'.

> **Note**
>
> Essa regra avalia apenas a última revisão ativa de uma definição de tarefa do Amazon ECS.

Identificador: ECS_TASK_DEFINITION_PID_MODE_CHECK

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

ecs-task-definition-user-for-host-mode-check

Verifica as permissões não autorizadas nas suas últimas definições de tarefa ativas do Amazon Elastic Container Service (Amazon ECS) que `NetworkMode` definiu para hospedar. A regra é NON_COMPLIANT para definições de tarefas com o `NetworkMode` definido como host e definições de contêiner de `privileged` definido como falso ou vazio e `user` definido como raiz ou vazio.

> **Important**
>
> Recomendamos que você remova privilégios elevados das definições de tarefas do Amazon ECS. Quando `privileged` verdadeiro, o contêiner recebe permissões elevadas na instância do contêiner hospedeiro (semelhante à do `root` usuário). Ao executar tarefas que usam o modo de rede `host`, não execute contêineres usando o usuário raiz (UID 0) para melhor segurança. Como uma prática recomendada de segurança, sempre utilize um usuário não raiz.

Identificador: ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

Tipos de recursos: AWS::ECS::TaskDefinition

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

SkipInactiveTaskDefinitions (Opcional), Tipo: booliano

Sinalizador booliano para não verificar as definições de tarefas INATIVAS do Amazon EC2. Se definida como 'true', a regra não avaliará as definições de tarefas INATIVAS do Amazon EC2. Se definida como 'false', a regra avaliará a revisão mais recente das definições de tarefas INATIVAS do Amazon EC2.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-access-point-enforce-root-directory

Verifica se os pontos de acesso do Amazon Elastic File System (Amazon EFS) estão configurados para impor um diretório raiz. A regra será NON_COMPLIANT se o valor de 'Path' for definido como '/' (diretório raiz padrão do sistema de arquivos).

Identificador: EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

Tipos de recursos: AWS::EFS::AccessPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

approvedDirectories (opcional), Tipo: Csv

Lista separada por vírgulas de caminhos de subdiretórios aprovados para a imposição do diretório raiz do ponto de acesso do Amazon EFS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-access-point-enforce-user-identity

Verifica se os pontos de acesso do Amazon Elastic File System (Amazon EFS) estão configurados para impor a identidade do usuário. A regra é NON_COMPLIANT se PosixUser " não estiver definido ou se os parâmetros forem fornecidos e não houver correspondência no parâmetro correspondente.

Identificador: EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

Tipos de recursos: AWS::EFS::AccessPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

approvedUids (opcional), Tipo: Csv

Lista separada por vírgulas de IDs de usuário POSIX aprovados para imposição de usuário do ponto de acesso de EFS.

approvedGids (opcional), Tipo: Csv

Lista separada por vírgulas de IDs de grupo POSIX aprovados para imposição de usuário do ponto de acesso de EFS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

efs-encrypted-check

Verifica se o Amazon Elastic File System (Amazon EFS) está configurado para criptografar os dados do arquivo usando AWS Key Management Service (AWS KMS). A regra será NON_COMPLIANT se a chave criptografada estiver definida como false em `DescribeFileSystems` ou se a chave `KmsKeyId` em `DescribeFileSystems` não corresponder ao parâmetro `KmsKeyId`.

Identifier (Identificador): EFS_ENCRYPTED_CHECK

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

KmsKeyId (Opcional), Tipo: string

Nome de recurso da Amazon (ARN) da chave do KMS usada para criptografar o sistema de arquivos do EFS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-in-backup-plan

Verifica se os sistemas de arquivos do Amazon Elastic File System (Amazon EFS) foram adicionados aos planos de backup do AWS Backup. A regra será NON_COMPLIANT se os sistemas de arquivos do EFS não estiverem incluídos nos planos de backup.

Identificador: EFS_IN_BACKUP_PLAN

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para sistemas de arquivos do Amazon Elastic File System (Amazon EFS). A regra será NON_COMPLIANT se o sistema de arquivos do Amazon EFS não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos sistemas de arquivos do Amazon EFS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do EFS para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-meets-restore-time-target

Confere se o tempo de restauração dos sistemas de arquivos Amazon Elastic File System (Amazon EFS) atende à duração especificada. A regra é NON_COMPLIANT se o sistema LatestRestoreExecutionTimeMinutes de arquivos do Amazon EFS for maior que minutos. maxRestoreTime

Identificador: EFS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags dos sistemas de arquivos do Amazon EFS para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do EFS para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-mount-target-public-accessible

Verifica se um destino de montagem do Amazon Elastic File System (Amazon EFS) não está associado a uma sub-rede pública. A regra NÃO ESTÁ EM CONFORMIDADE se o destino de montagem do Amazon EFS estiver associado a uma sub-rede pública.

Identificador: EFS_MOUNT_TARGET_PUBLIC_ACCESSIBLE

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

efs-resources-protected-by-backup-plan

Verifica se os sistemas de arquivos do Amazon Elastic File System (Amazon EFS) estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o sistema de arquivos do EFS não estiver coberto por um plano de backup.

Identificador: EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::EFS::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para sistemas de arquivos do EFS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do EFS para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eip-attached

Verifica se todos os endereços IP elásticos alocados a uma AWS conta estão vinculados às instâncias do EC2 ou às interfaces de rede elástica em uso. A regra é NON_COMPLIANT se o 'AssociationId' for nulo para o endereço IP elástico.

> **Note**
>
> Os resultados podem levar até 6 horas para estarem disponíveis após uma avaliação.

Identifier (Identificador): EIP_ATTACHED

Tipos de recursos: AWS::EC2::EIP

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
```

```
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-cluster-logging-enabled

Verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está configurado com o registro em log habilitado. A regra será NON_COMPLIANT se o registro em log dos clusters do Amazon EKS não estiver habilitado para todos os tipos de log.

Identificador: EKS_CLUSTER_LOGGING_ENABLED

Tipos de recursos: AWS::EKS::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-cluster-log-enabled

Verifica se um cluster do Amazon Elastic Kubernetes Service (Amazon EKS) está configurado com o registro em log habilitado. A regra será NON_COMPLIANT se o registro em log de clusters do Amazon EKS não estiver habilitado ou se o registro em log não estiver habilitado com o tipo de log mencionado.

Identificador: EKS_CLUSTER_LOG_ENABLED

Tipos de recursos: AWS::EKS::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

logTypes (opcional), Tipo: Csv

Lista separada por vírgulas dos tipos de log do ambiente de gerenciamento do EKS Cluster que devem ser habilitados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-cluster-oldest-supported-version

Verifica se um cluster do Amazon Elastic Kubernetes Service (EKS) está executando a versão mais antiga compatível. A regra será NON_COMPLIANT se um cluster do EKS estiver executando a versão mais antiga compatível (igual ao parâmetro "`oldestVersionSupported`).

Identificador: EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

Tipos de recursos: AWS::EKS::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mais antigo VersionSupported, Tipo: string

Valor da versão mais antiga do Kubernetes compatível com a AWS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-cluster-secrets-encrypted

Verifica se os clusters do Amazon EKS estão configurados para ter segredos do Kubernetes criptografados usando o KMS. AWS A regra é NON_COMPLIANT se um cluster EKS não tiver um recurso EncryptionConfig ou se EncryptionConfig não nomear segredos como um recurso.

Identificador: EKS_CLUSTER_SECRETS_ENCRYPTED

Tipos de recursos: AWS::EKS::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

> Lista separada por vírgula dos Amazon Resource Names (ARNs) da chave KMS que são aprovados para uso do EKS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

eks-cluster-supported-version

Verifica se um cluster do Amazon Elastic Kubernetes Service (EKS) está executando uma versão compatível do Kubernetes. Essa regra será NON_COMPLIANT se um cluster do EKS estiver executando uma versão não compatível (menor que o parâmetro '`oldestVersionSupported`').

Identificador: EKS_CLUSTER_SUPPORTED_VERSION

Tipos de recursos: AWS::EKS::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mais antigo VersionSupported, Tipo: string

Valor da versão mais antiga do Kubernetes compatível com a AWS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-endpoint-no-public-access

Verifica se o endpoint do Amazon Elastic Kubernetes Service (Amazon EKS) não está acessível ao público. A regra será NON_COMPLIANT se o endpoint estiver acessível publicamente.

Identificador: EKS_ENDPOINT_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::EKS::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

eks-secrets-encrypted

Verifica se os clusters do Amazon Elastic Kubernetes Service estão configurados para ter segredos do Kubernetes criptografados usando chaves (KMS). AWS Key Management Service

- Essa regra será COMPLIANT se um cluster do EKS tiver um encryptionConfig com segredos como um dos recursos.
- Essa regra também será COMPLIANT se a chave usada para criptografar segredos do EKS corresponder ao parâmetro.

- Essa regra será NON_COMPLIANT se um cluster do EKS não tiver um encryptionConfig ou se os recursos de encryptionConfig não tiverem segredos.
- Essa regra também é NON_COMPLIANT se a chave usada para criptografar segredos do EKS não corresponder ao parâmetro.

Identificador: EKS_SECRETS_ENCRYPTED

Tipos de recursos: AWS::EKS::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

Lista separada por vírgulas do nome do recurso da Amazon (ARN) da chave do KMS que deve ser usada para segredos criptografados em um cluster do EKS.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

elasticache-auto-minor-version-upgrade-check

Verifica se os clusters Amazon ElastiCache for Redis têm atualizações automáticas de versões secundárias habilitadas. A regra é NON_COMPLIANT para um ElastiCache cluster se ele estiver usando o mecanismo Redis e '' não estiver definido como AutoMinor VersionUpgrade 'verdadeiro'.

Identificador: ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

Tipos de recursos: AWS::ElastiCache::CacheCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-rbac-auth-enabled

Verifica se os grupos de ElastiCache replicação da Amazon têm a autenticação RBAC ativada. A regra é NON_COMPLIANT se a versão do Redis for 6 ou superior e os 'UserGroupIds' estiverem ausentes, vazios ou não corresponderem a uma entrada fornecida pelo parâmetro ". `allowedUserGroupIDs`

Identificador: ELASTICACHE_RBAC_AUTH_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

UserGroupIDs permitidos (opcional), Tipo: Csv

> Uma lista separada por vírgula de IDs de grupos de usuários aprovados para acesso ao grupo de ElastiCache replicação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-redis-cluster-automatic-backup-check

Verifique se os clusters do Amazon ElastiCache Redis têm o backup automático ativado. A regra é NON_COMPLIANT se o cluster SnapshotRetentionLimit for Redis for menor que o parâmetro. SnapshotRetentionPeriod Por exemplo: se o parâmetro for 15, a regra não estará em conformidade se snapshotRetentionPeriod estiver entre 0 e 15.

Identifier (Identificador): ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

Tipos de recursos: AWS::ElastiCache::CacheCluster, AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

snapshotRetentionPeriod (Opcional), Tipo: int, Padrão: 15

Período mínimo de retenção de snapshot em dias para o cluster do Redis. O padrão é 15 dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-repl-grp-auto-failover-enabled

Verifica se os grupos de replicação do Amazon ElastiCache Redis têm o failover automático ativado. A regra é NON_COMPLIANT para um grupo de ElastiCache replicação se '' não estiver definida como AutomaticFailover 'ativada'.

Identificador: ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-repl-grp-encrypted-at-rest

Verifica se os grupos de ElastiCache replicação da Amazon estão encryption-at-rest habilitados. A regra é NON_COMPLIANT para um grupo de ElastiCache replicação se 'AtRestEncryptionEnabled' estiver desativado ou se o ARN da chave KMS não corresponder ao parâmetro ApprovedKMS. KeyArns

Identificador: ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

KMS aprovado (opcional) KeyIds , Tipo: Csv

Lista separada por vírgula de IDs de chave KMS aprovadas para uso. ElastiCache

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

elasticache-repl-grp-encrypted-in-transit

Verifica se os grupos de ElastiCache replicação da Amazon estão encryption-in-transit habilitados. A regra é NON_COMPLIANT para um grupo de ElastiCache replicação se 'TransitEncryptionAtivado' estiver definido como 'false'.

Identificador: ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-repl-grp-redis-auth-enabled

Verifica se os grupos de ElastiCache replicação da Amazon têm o Redis AUTH ativado. A regra é NON_COMPLIANT para um grupo de ElastiCache replicação se a versão Redis de seus nós estiver abaixo de 6 (a versão 6+ usa ACLs do Redis) e '' estiver ausente ou estiver vazia/nula. AuthToken

Identificador: ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

Tipos de recursos: AWS::ElastiCache::ReplicationGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-subnet-group-check

Verifica se os ElastiCache clusters da Amazon estão configurados com um grupo de sub-rede personalizado. A regra é NON_COMPLIANT para um ElastiCache cluster se ele estiver usando um grupo de sub-rede padrão.

Identificador: ELASTICACHE_SUBNET_GROUP_CHECK

Tipos de recursos: AWS::ElastiCache::CacheCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticache-supported-engine-version

Verifica se os ElastiCache clusters estão executando uma versão maior ou igual à versão recomendada do mecanismo. A regra é NON_COMPLIANT se o 'EngineVersion' de um ElastiCache cluster for menor que a versão recomendada especificada para seu determinado mecanismo.

Identificador: ELASTICACHE_SUPPORTED_ENGINE_VERSION

Tipos de recursos: AWS::ElastiCache::CacheCluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mais recente MemcachedVersion, Tipo: string

A versão mais recente recomendada do mecanismo para o Memcached. Os valores válidos estão no formato de versionamento semântico (SemVer) com número de 3 componentes para versões principais, secundárias e de patch (por exemplo, 1.6.6, não 1.6).

mais recente RedisVersion, Tipo: string

A versão mais recente recomendada do mecanismo para o Redis. Os valores válidos estão no formato de versionamento semântico (SemVer) com número de 3 componentes para versões principais, secundárias e de patch (por exemplo, 7.0.5, não 7.0).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticsearch-encrypted-at-rest

Verifica se os domínios do Amazon OpenSearch Service (anteriormente chamados de Elasticsearch) têm a configuração de criptografia em repouso ativada. A regra é NON_COMPLIANT se o EncryptionAtRestOptions campo não estiver ativado.

Identifier (Identificador): ELASTICSEARCH_ENCRYPTED_AT_REST

Tipos de recursos: AWS::Elasticsearch::Domain

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

elasticsearch-in-vpc-only

Verifica se os domínios do Amazon OpenSearch Service (anteriormente chamados de Elasticsearch) estão na Amazon Virtual Private Cloud (Amazon VPC). A regra é NON_COMPLIANT se um endpoint de domínio OpenSearch de serviço for público.

Identifier (Identificador): ELASTICSEARCH_IN_VPC_ONLY

Tipos de recursos: AWS::Elasticsearch::Domain

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticsearch-logs-to-cloudwatch

Verifica se os domínios do Amazon OpenSearch Service estão configurados para enviar registros para o Amazon CloudWatch Logs. A regra será COMPLIANT se um log estiver habilitado para um domínio do Amazon ES. Essa regra será NON_COMPLIANT se o registro em log não estiver configurado.

Identificador: ELASTICSEARCH_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

logTypes (opcional), Tipo: Csv

> Lista separada por vírgulas de logs que estão habilitados. Os valores válidos são 'search', 'index', 'error'.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*Um objeto com uma ou mais das seguintes chaves: `SEARCH_SLOW_LOGS`, `ES_APPLICATION_LOGS`, `INDEX_SLOW_LOGS`, `AUDIT_LOGS`, dependendo dos tipos de logs que você deseja publicar. Cada chave precisa de um valor `LogPublishingOption` válido.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elasticsearch-node-to-node-encryption-check

Verifique se os nós do OpenSearch Service (anteriormente chamados de Elasticsearch) estão criptografados de ponta a ponta. A regra é NON_COMPLIANT se a node-to-node criptografia não estiver habilitada no domínio.

Identificador: ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipos de recursos: AWS::Elasticsearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elastic-beanstalk-logs-to-cloudwatch

Verifica se os ambientes do AWS Elastic Beanstalk estão configurados para enviar registros para o Amazon Logs. CloudWatch A regra é NON_COMPLIANT se o valor de `StreamLogs` for falso.

Identificador: ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

RetentionInDays (Opcional), Tipo: string

O número de dias que os eventos de log serão mantidos antes que expirem. Os valores válidos são: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653. A regra é NON_COMPLIANT se o valor de `logs. RetentionInDays` não corresponde a esse parâmetro.

DeleteOnTerminate (Opcional), Tipo: string

Verifica se os registros estão configurados para serem excluídos após o encerramento do ambiente. Os valores válidos são ‘verdadeiro’ ou ‘falso’. A regra é NON_COMPLIANT se o valor de `logs. DeleteOnTerminate` não corresponde a esse parâmetro.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elastic-beanstalk-managed-updates-enabled

Verifica se as atualizações gerenciadas da plataforma em um AWS Elastic Beanstalk ambiente estão habilitadas. A regra será COMPLIANT se o valor de `ManagedActionsEnabled` for definido como

verdadeiro. A regra será NON_COMPLIANT se o valor `ManagedActionsEnabled` for definido como falso, ou se um parâmetro for fornecido e seu valor não corresponder às configurações existentes.

Identificador: ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

Tipos de recursos: AWS::ElasticBeanstalk::Environment

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

UpdateLevel (Opcional), Tipo: string

Indica se os níveis de atualização estão definidos como atualizações de versão “secundárias” ou atualizações de versão de “patch”.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

elbv2-acm-certificate-required

Verifica se os Application Load Balancers e os Network Load Balancers têm ouvintes configurados para usar certificados do AWS Certificate Manager (ACM). Essa regra será NON-COMPLIANT se pelo menos 1 balanceador de carga tiver pelo menos 1 receptor configurado sem um certificado do ACM ou configurado com um certificado diferente de um certificado do ACM.

Identificador: ELBV2_ACM_CERTIFICATE_REQUIRED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

AcmCertificatesAllowed (Opcional), Tipo: Csv

Lista de certificados separada por vírgulas do Amazon Resource Names (ARNs).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elbv2-multiple-az

Verifica se um Elastic Load Balancer V2 (aplicação, rede ou Gateway Load Balancer) está mapeado para várias zonas de disponibilidade (AZs). A regra será NON_COMPLIANT se um Elastic Load Balancer V2 for mapeado para menos de dois AZs. Para obter mais informações, consulte Zonas de disponibilidade do seu Application Load Balancer.

Identificador: ELBV2_MULTIPLE_AZ

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

minAvailabilityZones (Opcional), Tipo: int

Número mínimo de AZs esperados (entre dois e dez inclusive).

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-acm-certificate-required

Verifica se os Classic Load Balancers usam certificados SSL fornecidos pelo. AWS Certificate Manager Para usar esta regra, use um listener SSL ou HTTPS com o Classic Load Balancer. Esta regra é aplicável somente aos Classic Load Balancers. Esta regra não verifica Application Load Balancers e Network Load Balancers.

Identifier (Identificador): ELB_ACM_CERTIFICATE_REQUIRED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-cross-zone-load-balancing-enabled

Verifica se o balanceamento de carga entre zonas está habilitado para Classic Load Balancers. A regra será NON_COMPLIANT se o balanceamento de carga entre zonas não estiver habilitado para Classic Load Balancers.

Identificador: ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-custom-security-policy-ssl-check

Verifica se os receptores SSL do Classic Load Balancer estão usando uma política personalizada. A regra é aplicável somente se houver receptores SSL para o Classic Load Balancer.

Identifier (Identificador): ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Cifras ssl ProtocolsAnd, Tipo: string

Lista separada por vírgulas de cifras e protocolos.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-deletion-protection-enabled

Verifica se o Elastic Load Balancer tem a proteção contra exclusão habilitada. A regra será NON_COMPLIANT se deletion_protection.enabled for falsa.

Identifier (Identificador): ELB_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-logging-enabled

Verifica se o Application Load Balancer e o Classic Load Balancer têm o registro em log habilitado. A regra é NON_COMPLIANT se `access_logs.s3.enabled` for falsa ou não `access_logs.S3.bucket` for igual ao s3 BucketName que você forneceu.

> **Note**
>
> A regra não se aplica a Network Load Balancers ou a Gateway Load Balancers.

Identifier (Identificador): ELB_LOGGING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

s3 BucketNames (opcional), Tipo: Csv

Lista separada por vírgulas de nomes de bucket do Amazon S3 para que o Amazon ELB entregue os arquivos de log.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-predefined-security-policy-ssl-check

Verifica se seus receptores SSL do Classic Load Balancer usam uma política predefinida. A regra será NON_COMPLIANT se a política do receptor do HTTPS/SSL do Classic Load Balancer não for igual ao valor do parâmetro ‘`predefinedPolicyName`‘.

Identifier (Identificador): ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

predefinido PolicyName, Tipo: string

O nome da política predefinida.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

elb-tls-https-listeners-only

Verifica se o Classic Load Balancer está configurado com receptores SSL ou HTTPS. A regra será NON_COMPLIANT se um receptor não estiver configurado com SSL ou HTTPS.

- Se o Classic Load Balancer não tiver um receptor configurado, a regra retornará NOT_APPLICABLE.
- A regra será COMPLIANT se os receptores do Classic Load Balancer estiverem configurados com SSL ou HTTPS.
- A regra será NON_COMPLIANT se um receptor não estiver configurado com SSL ou HTTPS.

Identificador: ELB_TLS_HTTPS_LISTENERS_ONLY

Tipos de recursos: AWS::ElasticLoadBalancing::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

emr-block-public-access

Verifica se uma conta com o Amazon EMR tem configurações de bloqueio de acesso público habilitadas. A regra é NON_COMPLIANT se BlockPublicSecurityGroupRules

for falsa ou, se verdadeira, portas diferentes da Porta 22 estiverem listadas em. PermittedPublicSecurityGroupRuleRanges

Identificador: EMR_BLOCK_PUBLIC_ACCESS

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

emr-kerberos-enabled

Verifica se os clusters do Amazon EMR têm Kerberos habilitado. A regra será NON_COMPLIANT se uma configuração de segurança não estiver anexada ao cluster ou se a configuração de segurança não atender aos parâmetros de regra especificados.

Identifier (Identificador): EMR_KERBEROS_ENABLED

Tipos de recursos: AWS::EMR::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

TicketLifetimeInHours (Opcional), Tipo: int

O período no qual o tíquete do Kerberos emitido pelo KDC do cluster permanece válido.

Realm (opcional), Tipo: string

O nome do realm do Kerberos do outro realm na relação de confiança.

Domínio (opcional), Tipo: string

O nome do domínio do outro realm na relação de confiança.

AdminServer (Opcional), Tipo: string

O domínio totalmente qualificado do servidor de administração no outro realm da relação de confiança.

KdcServer (Opcional), Tipo: string

O domínio totalmente qualificado do servidor do KDC no outro realm da relação de confiança.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

emr-master-no-public-ip

Verifica se os nós principais de clusters do Amazon EMR têm IPs públicos. A regra será NON_COMPLIANT se o nó principal tiver um IP público.

> **Note**
>
> Essa regra verifica os clusters que estão no estado RUNNING (Em execução) ou WAITING (Aguardando). Essa regra exige que você habilite a gravação do tipo de recurso do `AWS::EC2::Instance` para ter uma avaliação precisa.

Identifier (Identificador): EMR_MASTER_NO_PUBLIC_IP

Tipos de recursos: AWS::EMR::Cluster, AWS::EC2::Instance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

encrypted-volumes

Verifica se os volumes anexados do Amazon EBS estão criptografados e, opcionalmente, são criptografados com uma chave do KMS especificada. A regra será NON_COMPLIANT se os volumes anexados do EBS não estiverem criptografados ou forem criptografados com uma chave do KMS que não esteja nos parâmetros fornecidos.

Identifier (Identificador): ENCRYPTED_VOLUMES

Tipos de recursos: AWS::EC2::Volume

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsId (opcional), Tipo: string

ID ou ARN da chave KMS que é usada para criptografar o volume.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fms-shield-resource-policy-check

Verifica se um Application Load Balancer, CloudFront distribuições Amazon, Elastic Load Balancer ou Elastic IP tem proteção Shield. AWS Ele também verifica se eles têm uma ACL da web associada às distribuições do Application Load Balancer e da Amazon CloudFront .

Identifier (Identificador): FMS_SHIELD_RESOURCE_POLICY_CHECK

Tipos de recursos: AWS::CloudFront::Distribution, AWS::ElasticLoad BalancingV2::LoadBalancer, AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoad Balancing::,, LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

webACLId, Tipo: string

O WebACLId da ACL da web.

resourceTypes, Tipo: string

O escopo do recurso ao qual essa regra de configuração será aplicada.

resourceTags (opcional), Tipo: string

A tag de recurso à qual a regra deve ser associada (por exemplo, { "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }).

excludeResourceTags (Opcional), Tipo: booliano

Se for verdade, exclua os recursos que correspondem a resourceTags. Se for falso, inclua todos os recursos que correspondam a resourceTags.

fmsManagedToken (Opcional), Tipo: string

Um token gerado pelo AWS Firewall Manager ao criar a regra em sua conta. AWS Config ignora esse parâmetro quando você cria essa regra.

fmsRemediationEnabled (Opcional), Tipo: booliano

Se verdadeiro, o AWS Firewall Manager atualizará os recursos NON_COMPLIANT de acordo com a política do FMS. AWS Config ignora esse parâmetro quando você cria essa regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fms-webacl-resource-policy-check

Verifica se a ACL da web está associada a um Application Load Balancer, a um estágio do API Gateway ou a distribuições da Amazon CloudFront . Ao AWS Firewall Manager criar essa regra, o proprietário da política do FMS especifica a `WebACLId` na política do FMS e pode, opcionalmente, habilitar a remediação.

Identifier (Identificador): FMS_WEBACL_RESOURCE_POLICY_CHECK

Tipos de recursos AWS::CloudFront::Distribution, AWS::ApiGateway: :Stage, AWS::ElasticLoadBalancingV2::LoadBalancer, ACL AWS::WAFRegional::Web

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

webACLId, Tipo: string

O WebACLId da ACL da web.

resourceTags (opcional), Tipo: string

As tags de recursos (ApplicationLoadbalanceador ApiGatewayStage e CloudFront distribuições) às quais a regra deve ser associada. (por exemplo, {“tagKey1": [" tagValue1"], “tagKey2": [" tagValue2", “tagValue3"]})

excludeResourceTags (Opcional), Tipo: booliano

Se verdadeiro, exclui os recursos que correspondem a resourceTags.

fmsManagedToken (Opcional), Tipo: string

Um token gerado pelo AWS Firewall Manager ao criar a regra na conta do cliente. AWS Config ignora esse parâmetro quando o cliente cria essa regra.

fmsRemediationEnabled (Opcional), Tipo: booliano

Se verdadeiro, o AWS Firewall Manager atualizará os recursos não compatíveis de acordo com a política do FMS. AWS Config ignora esse parâmetro quando o cliente cria essa regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fms-webacl-rulegroup-association-check

Verifica se os grupos de regras estão associados com a ACL da web na prioridade correta. A prioridade correta é decidida pela classificação dos grupos de regras no parâmetro ruleGroups.

Quando AWS Firewall Manager cria essa regra, ela atribui a prioridade mais alta 0 seguida por 1, 2 e assim por diante. O proprietário da política do FMS especifica a classificação `ruleGroups` na política do FMS e pode habilitar as correções.

Identifier (Identificador): FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Tipos de recursos: AWS::WAF::Web ACL, AWS::WAFRegional::Web ACL

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

ruleGroups, Tipo: string

Lista separada por vírgulas de RuleGroupIds e WafOverrideAction pares. (por exemplo, ruleGroupId -1:NONE, ruleGroupId 2:COUNT)

fmsManagedToken (Opcional), Tipo: string

Um token gerado pelo AWS Firewall Manager ao criar a regra na conta do cliente. AWS Config ignora esse parâmetro quando o cliente cria essa regra.

fmsRemediationEnabled (Opcional), Tipo: booliano

Se verdadeiro, o AWS Firewall Manager atualizará os recursos não compatíveis de acordo com a política do FMS. AWS Config ignora esse parâmetro quando o cliente cria essa regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation].

fsx-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para o sistema de arquivos do Amazon FSx. A regra será NON_COMPLIANT se o sistema de arquivos do Amazon FSx não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos sistemas de arquivos do Amazon FSx para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do Amazon FSx para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fsx-lustre-copy-tags-to-backups

Verifica se os sistemas de arquivos do Amazon FSx para Lustre estão configurados para copiar tags para backups. A regra será NON_COMPLIANT se os sistemas de arquivos do Lustre não estiverem configurados para copiar tags para backups.

Identificador: FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fsx-meets-restore-time-target

Confere se o tempo de restauração dos sistemas de arquivos Amazon FSx atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes um sistema de arquivos Amazon FSx for maior que minutos. maxRestoreTime

Identificador: FSX_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags dos sistemas de arquivos do Amazon FSx para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do Amazon FSx para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fsx-openzfs-copy-tags-enabled

Verifica se os sistemas de arquivos do Amazon FSx para OpenZFS estão configurados para copiar tags para backups e volumes. A regra será NON_COMPLIANT se os sistemas de arquivos FSx para OpenZFS não estiverem configurados para copiar tags para backups e volumes.

Identificador: FSX_OPENZFS_COPY_TAGS_ENABLED

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na Europa (Estocolmo), Ásia-Pacífico (Mumbai), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), Ásia-Pacífico (Hong Kong), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney), Canadá (Central)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fsx-resources-protected-by-backup-plan

Verifica se os sistemas de arquivos do Amazon FSx estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o sistema de arquivos do Amazon FSx não estiver coberto por um plano de backup.

Identificador: FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos sistemas de arquivos do Amazon FSx para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do sistema de arquivos do Amazon FSx para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

fsx-windows-audit-log-configured

Verifica se os sistemas de arquivos do Amazon FSx para Windows File Server têm a auditoria de acesso a arquivos habilitada. A regra será NON_COMPLIANT se os sistemas de arquivos do FSx para Windows File Server não tiverem a auditoria de acesso a arquivos habilitada.

Identificador: FSX_WINDOWS_AUDIT_LOG_CONFIGURED

Tipos de recursos: AWS::FSx::FileSystem

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

global-endpoint-event-replication-enabled

Verifica se a replicação de eventos está habilitada para endpoints EventBridge globais da Amazon. A regra será NON_COMPLIANT se a replicação do evento não estiver habilitada.

Identificador: GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

Tipos de recursos: AWS::Events::Endpoint

Tipo de trigger: alterações da configuração

Região da AWS: Disponível somente na Europa (Estocolmo), Ásia-Pacífico (Mumbai), Europa (Paris), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), América do Sul (São Paulo), Leste dos EUA (Norte da Virgínia), Ásia-Pacífico (Seul), Ásia-Pacífico (Osaka), Ásia-Pacífico (Cingapura)), região Ásia-Pacífico (Sydney), Canadá (Central)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

guardduty-eks-protection-audit-habilitado

Verifica se o monitoramento do log de auditoria do Amazon Elastic Kubernetes Service (Amazon EKS) está ativado para um detector da GuardDuty Amazon em sua conta. A regra é NON_COMPLIANT se o recurso EKS Audit Log Monitoring não estiver habilitado para sua conta.

Identificador: GUARDDUTY_EKS_PROTECTION_AUDIT_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

guardduty-eks-protection-runtime-habilitado

Verifica se o Amazon EKS Runtime Monitoring com gerenciamento automatizado de agentes está habilitado para GuardDuty detector em sua conta. A regra é NON_COMPLIANT se o EKS Runtime Monitoring com gerenciamento automatizado de agentes não GuardDuty estiver habilitado para sua conta.

Identificador: GUARDDUTY_EKS_PROTECTION_RUNTIME_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

guardduty-enabled-centralized

Verifica se a Amazon GuardDuty está habilitada em sua AWS conta e AWS região. Se você fornecer uma AWS conta para centralização, a regra avaliará os GuardDuty resultados na conta centralizada. A regra é COMPATÍVEL quando GuardDuty está ativada.

Identifier (Identificador): GUARDDUTY_ENABLED_CENTRALIZED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

CentralMonitoringAccount (Opcional), Tipo: string

Lista de AWS contas separada por vírgula (12 dígitos) em que GuardDuty os resultados da Amazon podem ser centralizados.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para proteção guardduty-lambda

Verifica se o Lambda Protection está habilitado para um GuardDuty detector Amazon em sua conta. A regra não é compatível se o recurso de Proteção Lambda na Amazon não GuardDuty estiver habilitado para sua conta.

Identificador: GUARDDUTY_LAMBDA_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

proteção contra malware guardduty-habilitada

Verifica se a Proteção contra Malware está ativada para um GuardDuty detector da Amazon em sua conta. A regra é NON_COMPLIANT se o recurso de proteção contra malware na Amazon não GuardDuty estiver habilitado para sua conta.

Identificador: GUARDDUTY_MALWARE_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

guardduty-non-archived-findings

Verifica se a Amazon GuardDuty tem descobertas que não estão arquivadas. A regra é NON_COMPLIANT se GuardDuty tiver resultados de severidade baixa/média/alta não arquivados anteriores ao número especificado no parâmetro /days /. daysLowSev MediumSev `daysHighSev`

Identifier (Identificador): GUARDDUTY_NON_ARCHIVED_FINDINGS

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

daysLowSev (Opcional), Tipo: int, Padrão: 30

O número de dias em que as descobertas de GuardDuty baixa severidade da Amazon podem permanecer não arquivadas. O padrão são 30 dias.

daysMediumSev (Opcional), Tipo: int, Padrão: 7

O número de dias em que as descobertas de severidade GuardDuty média da Amazon podem permanecer não arquivadas. O padrão são 7 dias.

daysHighSev (Opcional), Tipo: int, Padrão: 1

O número de dias em que as descobertas GuardDuty de alta severidade da Amazon podem permanecer não arquivadas. O padrão é 1 dia.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

proteção guardduty-rds-habilitada

Verifica se a proteção do Amazon Relational Database Service (Amazon RDS) está ativada para um detector da GuardDuty Amazon em sua conta. A regra é NON_COMPLIANT se o recurso de proteção do Amazon RDS na Amazon não GuardDuty estiver habilitado para sua conta.

Identificador: GUARDDUTY_RDS_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

proteção guardduty-s3 ativada

Verifica se o S3 Protection está habilitado para um Amazon GuardDuty Detector em sua conta. A regra é NON_COMPLIANT se o recurso de proteção do S3 na Amazon não GuardDuty estiver habilitado para sua conta.

Identificador: GUARDDUTY_S3_PROTECTION_ENABLED

Tipos de recursos: AWS::GuardDuty::Detector

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-customer-policy-blocked-kms-actions

Verifica se as políticas gerenciadas de AWS Identity and Access Management (IAM) criadas por você não permitem ações bloqueadas AWS nas chaves KMS. A regra é NON_COMPLIANT se alguma ação bloqueada for permitida nas chaves AWS KMS pela política gerenciada do IAM.

> **Note**
>
> Essa regra não avalia variáveis ou condições nas políticas do IAM. Para obter mais informações, consulte Elementos da política do IAM: Variáveis e elementos da política JSON do IAM: condição no Guia do usuário do IAM.

Identificador: IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

Tipos de recursos: AWS::IAM::Policy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

bloqueado ActionsPatterns, Tipo: Csv

Lista separada por vírgulas de padrões de ação bloqueados do KMS. Por exemplo, você pode listar kms:decrypt* ou kms: como padrões de ação bloqueados. ReEncrypt A regra será NON_COMPLIANT se a política gerenciada do IAM permitir qualquer padrão de ação listado nesse parâmetro.

excluir PermissionBoundaryPolicy (opcional), Tipo: booliano

Sinalizador booleano para excluir a avaliação das políticas do IAM usadas como limites de permissões. Se definida como 'true', a regra não incluirá limites de permissões na avaliação.

Caso contrário, todas as políticas do IAM no escopo são avaliadas quando o valor é definido como ‘falso’. O valor padrão é ‘false’.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-external-access analyzer ativado

Verifica se um IAM Access Analyzer para acesso externo está ativado em sua conta por região. A regra é NON_COMPLIANT se não houver analisadores para acesso externo na região ou se o atributo 'status' não estiver definido como 'ATIVO'.

Identificador: IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-group-has-users-check

Verifica se os grupos do IAM têm, pelo menos, um usuário do IAM.

Identifier (Identificador): IAM_GROUP_HAS_USERS_CHECK

Tipos de recursos: AWS::IAM::Group

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-inline-policy-blocked-kms-actions

Verifica se as políticas embutidas anexadas aos seus usuários, funções e grupos do IAM não permitem ações bloqueadas em todas as chaves do AWS KMS. A regra é NON_COMPLIANT se alguma ação bloqueada for permitida em todas as chaves AWS KMS em uma política em linha.

Identificador: IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

Tipos de recursos: AWS::IAM::Group, AWS::IAM::Role, AWS::IAM::User

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

bloqueado ActionsPatterns, Tipo: Csv

Lista separada por vírgulas de padrões de ação do KMS bloqueados, por exemplo, kms: *, kms:Decrypt, kms: *. ReEncrypt

excluir RoleByManagementAccount (opcional), Tipo: booliano

Exclua uma função se ela só puder ser assumida pela conta de gerenciamento da organização.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-no-inline-policy-check

Verifica se o recurso de política em linha não está em uso. A regra não é compatível se um usuário do AWS Identity and Access Management (IAM), uma função do IAM ou um grupo do IAM tiver alguma política em linha.

Identificador: IAM_NO_INLINE_POLICY_CHECK

Tipos de recursos: AWS::IAM::User, AWS::IAM::Role, AWS::IAM::Group

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

iam-password-policy

Verifica se a política de senha da conta para usuários do AWS Identity and Access Management (IAM) atende aos requisitos especificados nos parâmetros. A regra será NON_COMPLIANT se a política de senha da conta não atender aos requisitos especificados.

> **Important**
>
> Os valores `true` e `false` dos parâmetros da regra diferenciam maiúsculas de minúsculas. Se `true` não estiver em letras minúsculas, será tratado como `false`.

> **Note**
>
> Resultado da avaliação da política de senha padrão do IAM
> Essa regra é marcada como NON_COMPLIANT quando a política de senha padrão do IAM é usada.

Regras gerenciadas e tipos de recursos globais do IAM
Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): IAM_PASSWORD_POLICY

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

RequireUppercaseCharacters (Opcional), Tipo: booliano, Padrão: True

Exige pelo menos um caractere maiúsculo na senha.

RequireLowercaseCharacters (Opcional), Tipo: booliano, Padrão: True

Exige pelo menos um caractere minúsculo na senha.

RequireSymbols (Opcional), Tipo: booliano, Padrão: True

Exige pelo menos um símbolo na senha.

RequireNumbers (Opcional), Tipo: booliano, Padrão: True

Exige pelo menos um número na senha.

MinimumPasswordLength (Opcional), Tipo: int, Padrão: 14

Tamanho mínimo da senha.

PasswordReusePrevention (Opcional), Tipo: int, Padrão: 24

Número de senhas antes de permitir a reutilização.

MaxPasswordAge (Opcional), Tipo: int, Padrão: 90

Número de dias antes da expiração da senha.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-policy-blacklisted-check

Verifica em cada recurso do AWS Identity and Access Management (IAM) se uma política Amazon Resource Name (ARN) no parâmetro de entrada está anexada ao recurso do IAM. A regra será NON_COMPLIANT se o ARN da política for vinculado ao recurso do IAM.

Identifier (Identificador): IAM_POLICY_BLACKLISTED_CHECK

Tipos de recursos: AWS::IAM::User, AWS::IAM::Group, AWS::IAM::Role

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

policyArns, Tipo: Csv, Padrão: arn:aws:iam: :aws:policy/ AdministratorAccess

Lista separada por vírgulas de avisos de política do IAM que não devem ser anexados a nenhuma entidade do IAM.

exceptionList (opcional), Tipo: Csv

Lista separada por vírgula de tipos de recursos e lista de pares de nomes de recursos. Por exemplo, usuários:[usuário1;usuário2], grupos:[grupo1;grupo2], funções: [função1;função2;função3].

> **Note**
>
> Para a lista de exceções, especifique o nome do recurso e não o ARN completo. Não é válido:`arn:aws:iam::444455556666:role/Admin`. Válido:`Admin`.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-policy-in-use

Verifica se o ARN da política do IAM está vinculado a um usuário do IAM ou a um grupo com um ou mais usuários do IAM, ou um perfil do IAM com uma ou mais entidades confiáveis.

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
> Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
> Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identificador: IAM_POLICY_IN_USE

Tipos de recursos: AWS::IAM::Policy

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

policyARN, Tipo: string

Um ARN da política do IAM a ser verificado.

policyUsageType (Opcional), Tipo: string

Especifique se você quer que a política seja anexada a um usuário, grupo ou perfil do IAM. Os valores válidos são IAM_USER, IAM_GROUP, IAM_ROLE ou ANY. O valor padrão é ANY.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-policy-no-statements-with-admin-access

Verifica se as políticas de AWS Identity and Access Management (IAM) criadas por você têm instruções Allow que concedem permissões para todas as ações em todos os recursos. A regra será NON_COMPLIANT se alguma declaração de política do IAM incluir "Effect": "Allow" with "Action": "*" over "Resource": "*".

> **Note**
>
> Essa regra avalia somente as políticas gerenciadas pelo cliente. Essa regra NÃO avalia políticas embutidas ou políticas AWS gerenciadas. Para obter mais informações sobre a diferença, consulte Políticas gerenciadas e em linha no Guia do Usuário do IAM.

A seguinte política é NON_COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
```

```
}
```

A seguinte política é COMPLIANT:

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

Identifier (Identificador): IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

Tipos de recursos: AWS::IAM::Policy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

excluir PermissionBoundaryPolicy (opcional), Tipo: booliano

> Sinalizador booleano para excluir a avaliação das políticas do IAM usadas como limites de permissões. Se definida como 'true', a regra não incluirá limites de permissões na avaliação. Caso contrário, todas as políticas do IAM no escopo são avaliadas quando o valor é definido como ‘falso’. O valor padrão é ‘false’.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

iam-policy-no-statements-with-full-access

Verifica se as políticas de AWS Identity and Access Management (IAM) criadas por você concedem permissões para todas as ações em AWS recursos individuais. A regra é NON_COMPLIANT se alguma política de IAM gerenciada pelo cliente permitir acesso total a pelo menos um serviço. AWS

Contexto: seguindo o princípio do menor privilégio, é recomendável limitar as ações permitidas em suas políticas do IAM ao conceder permissões aos AWS serviços. Essa abordagem ajuda a garantir

que você conceda somente as permissões necessárias especificando as ações exatas necessárias, evitando o uso de curingas irrestritos para um serviço, como. `ec2:*`

Em alguns casos, talvez você queira permitir várias ações com um prefixo semelhante, como DescribeFlowregistros e DescribeAvailabilityzonas. Nesses casos, você pode adicionar um caractere curinga com sufixo ao prefixo comum (por exemplo,). `ec2:Describe*` O agrupamento de ações relacionadas pode ajudar a evitar atingir os limites de tamanho da política do IAM.

Essa regra retornará COMPATÍVEL se você usar ações prefixadas com um caractere curinga com sufixo (por exemplo,). `ec2:Describe*` Essa regra só retornará NON_COMPLIANT se você usar curingas irrestritos (por exemplo,). `ec2:*`

> **Note**
>
> Essa regra avalia somente as políticas gerenciadas pelo cliente. Essa regra NÃO avalia políticas embutidas ou políticas AWS gerenciadas. Para obter mais informações sobre a diferença, consulte Políticas gerenciadas e em linha no Guia do Usuário do IAM.

Identificador: IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

Tipos de recursos: AWS::IAM::Policy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

excluir PermissionBoundaryPolicy (opcional), Tipo: booliano

> Sinalizador booleano para excluir a avaliação das políticas do IAM usadas como limites de permissões. Se definida como 'true', a regra não incluirá limites de permissões na avaliação. Caso contrário, todas as políticas do IAM no escopo são avaliadas quando o valor é definido como ‘falso’. O valor padrão é ‘false’.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-role-managed-policy-check

Verifica se todas as políticas gerenciadas especificadas na lista de políticas gerenciadas estão anexadas à função AWS Identity and Access Management (IAM). A regra será NON_COMPLIANT se uma política gerenciada não estiver associada ao perfil do IAM.

Identifier (Identificador): IAM_ROLE_MANAGED_POLICY_CHECK

Tipos de recursos: AWS::IAM::Role

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

gerenciado PolicyArns, Tipo: Csv

> Lista separada por vírgula de Amazon Resource Names (ARNs) de políticas AWS gerenciadas. Para obter mais informações, consulte nomes do recurso da Amazon (ARN) e políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-root-access-key-check

Verifica se a chave de acesso do usuário raiz está disponível. A regra será COMPLIANT se a chave de acesso do usuário não existir. Caso contrário, NON_COMPLIANT.

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): IAM_ROOT_ACCESS_KEY_CHECK

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

verificação de expiração do certificado do servidor iam

Verifica se os certificados de servidor SSL/TLS do AWS IAM armazenados no IAM expiraram. A regra é NON_COMPLIANT se um certificado de servidor IAM expirar.

Identificador: IAM_SERVER_CERTIFICATE_EXPIRATION_CHECK

Tipos de recursos: AWS::IAM::ServerCertificate

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-user-group-membership-check

Verifica se os usuários IAM são membros de pelo menos um grupo do IAM.

Identifier (Identificador): IAM_USER_GROUP_MEMBERSHIP_CHECK

Tipos de recursos: AWS::IAM::User

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

groupNames (opcional), Tipo: string

Lista separada por vírgulas dos grupos do IAM dos quais os usuários do IAM devem ser membros.

> **Note**
>
> Esta regra não é compatível com nomes de grupo com vírgulas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-user-mfa-enabled

Verifica se os usuários do AWS Identity and Access Management (IAM) têm a autenticação multifator (MFA) ativada. A regra será NON_COMPLIANT se a MFA não estiver habilitada para pelo menos um usuário do IAM.

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): IAM_USER_MFA_ENABLED

Tipos de recursos: AWS::IAM::User

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-user-no-policies-check

Verifica se nenhum dos seus usuários do AWS Identity and Access Management (IAM) tem políticas anexadas. Os usuários do IAM devem herdar permissões dos grupos ou funções do IAM. A regra será NON_COMPLIANT se houver pelo menos um usuário do IAM com políticas anexadas.

Identifier (Identificador): IAM_USER_NO_POLICIES_CHECK

Tipos de recursos: AWS::IAM::User

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

iam-user-unused-credentials-check

Verifica se seus usuários AWS Identity and Access Management (IAM) têm senhas ou chaves de acesso ativas que não foram usadas no número especificado de dias que você forneceu. A regra será NON_COMPLIANT se houver contas inativas que não foram usadas recentemente.

> **Note**
>
> Cronograma de reavaliação
> Reavaliar essa regra em até 4 horas após a primeira avaliação não terá efeito sobre os resultados.
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
> Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): IAM_USER_UNUSED_CREDENTIALS_CHECK

Tipos de recursos: AWS::IAM::User

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

CredentialUsageIdade máxima, Tipo: int, Padrão: 90

Número máximo de dias em que uma credencial não pode ser usada. O valor padrão é 90 dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

restricted-ssh

Important

Para essa regra, o identificador da regra (INCOMING_SSH_DISABLED) e o nome da regra (restricted-ssh) são diferentes.

Verifica se o tráfego de entrada SSH dos grupos de segurança é acessível. A regra será COMPLIANT se os endereços IP do tráfego de entrada SSH nos grupos de segurança forem restritos (CIDR diferente de 0.0.0.0/0 ou ::/0). Caso contrário, NON_COMPLIANT.

Identifier (Identificador): INCOMING_SSH_DISABLED

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

inspetor-ec2-scan habilitado

Verifica se a verificação EC2 do Amazon Inspector V2 está ativada para seu ambiente de uma ou várias contas para detectar possíveis vulnerabilidades e problemas de acessibilidade de rede em suas instâncias do EC2. A regra é NON_COMPLIANT se a varredura do EC2 não estiver ativada.

Identificador: INSPECTOR_EC2_SCAN_ENABLED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para inspector-ecr-scan

Verifica se o escaneamento ECR do Amazon Inspector V2 está ativado em seu ambiente de uma ou várias contas para detectar possíveis vulnerabilidades de software nas imagens do seu contêiner. A regra é NON_COMPLIANT se o escaneamento ECR não estiver ativado.

Identificador: INSPECTOR_ECR_SCAN_ENABLED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para escaneamento de código lambda do inspetor

Verifica se a digitalização de código Lambda do Amazon Inspector V2 está ativada em seu ambiente de uma ou várias contas para detectar possíveis vulnerabilidades de código. A regra é NON_COMPLIANT se a digitalização de código Lambda não estiver ativada.

Identificador: INSPECTOR_LAMBDA_CODE_SCAN_ENABLED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Disponível somente na Europa (Estocolmo), Leste dos EUA (Ohio), Europa (Irlanda), Europa (Frankfurt), Leste dos EUA (Norte da Virgínia), Europa (Londres), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

habilitado para escaneamento padrão inspetor-lambda

Verifica se o escaneamento padrão do Amazon Inspector V2 Lambda está ativado em seu ambiente de uma ou várias contas para detectar possíveis vulnerabilidades de software. A regra é NON_COMPLIANT se o escaneamento padrão do Lambda não estiver ativado.

Identificador: INSPECTOR_LAMBDA_STANDARD_SCAN_ENABLED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ec2-instances-in-vpc

> **Important**
>
> Para essa regra, o identificador da regra (INSTANCES_IN_VPC) e o nome da regra (ec2-instances-in-vpc) são diferentes.

Verifica se suas instâncias do EC2 pertencem a uma nuvem privada virtual (VPC). Opcionalmente, você pode especificar o ID da VPC para associar com suas instâncias.

Identifier (Identificador): INSTANCES_IN_VPC

Tipos de recursos: AWS::EC2::Instance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

vpcId (opcional), Tipo: string

O ID da VPC que contém essas instâncias do EC2.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

internet-gateway-authorized-vpc-only

Verifica se os gateways da Internet estão conectados a uma nuvem privada virtual autorizada (Amazon VPC). A regra será NON_COMPLIANT se os gateways da Internet estiverem conectados a uma VPC não autorizada.

Identifier (Identificador): INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

Tipos de recursos: AWS::EC2::InternetGateway

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

AuthorizedVpcIds (Opcional), Tipo: string

Lista separada por vírgulas dos IDs de VPC autorizadas com IGWs associados. Se o parâmetro não for fornecido, todos os IGWs associados serão NON_COMPLIANT.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

kinesis-firehose-delivery-stream criptografado

Verifica se os streams de entrega do Amazon Kinesis Data Firehose estão criptografados em repouso com criptografia do lado do servidor. A regra é NON_COMPLIANT se um stream de entrega do Kinesis Data Firehose não for criptografado em repouso com criptografia do lado do servidor.

Identificador: KINESIS_FIREHOSE_DELIVERY_STREAM_ENCRYPTED

Tipos de recursos: AWS::KinesisFirehose::DeliveryStream

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

Lista separada por vírgula dos KMS Key Arns aprovados para uso do Kinesis Firehose.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

kinesis-stream-encrypted

Verifica se os fluxos do Amazon Kinesis foram criptografados em repouso com a criptografia do lado do servidor. A regra é NON_COMPLIANT para um stream do Kinesis se '' não estiver presente. StreamEncryption

Contexto: A criptografia do lado do servidor é um recurso do Amazon Kinesis Data Streams que criptografa automaticamente os dados antes que estejam em repouso usando uma chave KMS. AWS Os dados são criptografados antes de serem gravados na camada de armazenamento do fluxo do Kinesis e descriptografados depois de recuperados do armazenamento. Como resultado, os dados são criptografados em repouso no serviço Kinesis Data Streams. Isso permite que você atenda a requisitos normativos rígidos e aprimore a segurança de seus dados. Para obter mais informações, consulte [Proteção de dados no Amazon Kinesis Data Streams](#).

Identificador: KINESIS_STREAM_ENCRYPTED

Tipos de recursos: AWS::Kinesis::Stream

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

kms-cmk-not-scheduled-for-deletion

Verifica se as chaves do AWS Key Management Service (AWS KMS) não estão programadas para exclusão no AWS KMS. A regra é NON_COMPLIANT se as chaves KMS estiverem programadas para exclusão.

Identifier (Identificador): KMS_CMK_NOT_SCHEDULED_FOR_DELETION

Tipos de recursos: AWS::KMS::Key

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyIds (Opcional), Tipo: string

> (Opcional) Lista separada por vírgulas de IDs específicos de chave gerenciada pelo cliente que não devem ser agendados para exclusão. Se nenhuma chave for especificada, a regra verificará todas elas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-concurrency-check

Verifica se a função do Lambda está configurada com o limite de execuções simultâneas em nível de função. A regra será NON_COMPLIANT se a função do Lambda não estiver configurada com o limite de execuções simultâneas em nível de função.

Identifier (Identificador): LAMBDA_CONCURRENCY_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

ConcurrencyLimitLow (Opcional), Tipo: string

Limite mínimo de execuções de simultaneidade

ConcurrencyLimitHigh (Opcional), Tipo: string

Limite máximo de execuções de simultaneidade

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-dlq-check

Verifica se uma função do Lambda está configurada com uma fila de mensagens não entregues. A regra será NON_COMPLIANT se a função do Lambda não estiver configurada com uma fila de mensagens não entregues.

Identifier (Identificador): LAMBDA_DLQ_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

dlqArns (opcional), Tipo: string

Lista separada por vírgulas de ARNs do Amazon SQS e Amazon SNS que devem ser configurados como o destino da fila de mensagens não entregues da função do Lambda.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-function-public-access-prohibited

Verifica se a política de AWS Lambda função anexada ao recurso Lambda proíbe o acesso público. Se a política de função do Lambda permitir o acesso público, será NON_COMPLIANT.

Contexto: considera-se que uma política de função lambda permite acesso público se o elemento principal estiver vazio ou contiver um curinga. Por exemplo, se o elemento principal for `“”` ou`{“AWS”: “”}`. Não é recomendável conceder acesso público por motivos de segurança. Restringir o acesso público pode ajudar você a evitar invocações não autorizadas de suas funções do Lambda, o que pode comprometer seus dados ou gerar custos indesejados.

Para restringir o acesso às suas funções do Lambda, especifique os IDs da AWS conta ou os Amazon Resource Names (ARNs) dos usuários, funções ou serviços do IAM que podem invocar as funções. Para obter mais informações, consulte Conceder acesso funcional a outras contas no Guia do AWS Lambda desenvolvedor.

Identifier (Identificador): LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-function-settings-check

Verifica se as configurações AWS da função Lambda para tempo de execução, função, tempo limite e tamanho da memória correspondem aos valores esperados. A regra ignora funções com o tipo de pacote “Imagem” e funções com tempo de execução definido como “Tempo de execução somente do sistema operacional”. A regra será NON_COMPLIANT se as configurações da função do Lambda não corresponderem aos valores esperados.

Identifier (Identificador): LAMBDA_FUNCTION_SETTINGS_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

runtime, Tipo: Csv

Lista separada por vírgula dos valores de tempo de execução do Lambda AWS

função (opcional), Tipo: string

Nome ou ARN da função de execução do Lambda AWS

timeout (opcional), Tipo: int, Padrão: 3

AWS Tempo limite da função Lambda em segundos

memorySize (opcional), Tipo: int, Padrão: 128

AWS Tamanho da função Lambda em megabytes

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* Para obter mais informações sobre valores válidos para essas entradas, consulte Função MemorySize, Tempo de Execução e Tempo Limite no Guia do AWS CloudFormation Usuário.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-inside-vpc

Verifica se uma função do Lambda tem permissão para acessar uma nuvem privada virtual (VPC). A regra será NON_COMPLIANT se a função do Lambda não estiver em uma VPC.

Identifier (Identificador): LAMBDA_INSIDE_VPC

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

subnetIds (opcional), Tipo: string

> Lista separada por vírgulas de IDs de sub-rede aos quais as funções do Lambda devem ser associadas.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

lambda-vpc-multi-az-check

Verifica se o Lambda tem mais de uma zona de disponibilidade associada. A regra será NON_COMPLIANT se apenas 1 zona de disponibilidade estiver associada ao Lambda ou se o número de zonas de disponibilidade associadas for menor que o número especificado no parâmetro opcional.

Identificador: LAMBDA_VPC_MULTI_AZ_CHECK

Tipos de recursos: AWS::Lambda::Function

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

availabilityZones (opcional), Tipo: int

Número de zonas de disponibilidade esperadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

verificação automática de descoberta de dados com sensibilidade automática

Verifica se a descoberta automatizada de dados confidenciais está habilitada para o Amazon Macie. A regra é NON_COMPLIANT se a descoberta automática de dados confidenciais estiver desativada. A regra é APLICÁVEL para contas de administrador e NOT_APPLICABLE para contas de membros.

Identificador: MACIE_AUTO_SENSITIVE_DATA_DISCOVERY_CHECK

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

macie-status-check

Verifica se o Amazon Macie está habilitado em sua conta por região. A regra será NON_COMPLIANT se o atributo 'status' não estiver definido como 'ENABLED'.

Identificador: MACIE_STATUS_CHECK

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mfa-enabled-for-iam-console-access

Verifica se a autenticação AWS multifator (MFA) está habilitada para AWS todos os usuários do Identity and Access Management (IAM) que usam uma senha de console. A regra será COMPLIANT se a MFA estiver habilitada.

> **Note**
>
> Cronograma de reavaliação
> Reavaliar essa regra em até 4 horas após a primeira avaliação não terá efeito sobre os resultados.

Regras gerenciadas e tipos de recursos globais do IAM
Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

Tipos de recursos: AWS::IAM::User

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-active-deployment-mode

Verifica o modo de implantação configurado para o mecanismo de agente ActiveMQ do Amazon MQ. A regra é NON_COMPLIANT se o modo de agente de instância única padrão estiver sendo usado.

Identificador: MQ_ACTIVE_DEPLOYMENT_MODE

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-automatic-minor-version-upgrade-enabled

Verifica se atualizações automáticas de versões secundárias estão habilitadas para agentes do Amazon MQ. A regra é NON_COMPLIANT se o campo 'AutoMinorVersionUpgrade' não estiver habilitado para um agente do Amazon MQ.

Identificador: MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-auto-minor-version-upgrade-enabled

Verifica se atualizações automáticas de versões secundárias estão habilitadas para agentes do Amazon MQ. A regra é NON_COMPLIANT se o campo 'AutoMinorVersionUpgrade' não estiver habilitado para um agente do Amazon MQ.

Identificador: MQ_AUTO_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

mq-cloudwatch-audit-logging-enabled

Verifica se os corretores do Amazon MQ têm o registro de CloudWatch auditoria da Amazon ativado. A regra é NON_COMPLIANT se um agente não tiver o registro em log de auditoria habilitado.

Identificador: MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-cloudwatch-audit-log-habilitado

Verifica se um agente do Amazon MQ tem o registro de CloudWatch auditoria ativado. A regra é NON_COMPLIANT se o agente não tiver o registro de auditoria ativado.

Identificador: MQ_CLOUDWATCH_AUDIT_LOG_ENABLED

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-no-public-access

Verifica se os agentes do Amazon MQ não estão acessíveis ao público. A regra é NON_COMPLIANT se o campo 'PubliclyAccessible' for definido como verdadeiro para um agente do Amazon MQ.

Identificador: MQ_NO_PUBLIC_ACCESS

Tipos de recursos: AWS::AmazonMQ::Broker

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

mq-rabbit-deployment-mode

Verifica o modo de implantação configurado para o mecanismo de agente do Amazon MQ RabbitMQ. A regra é NON_COMPLIANT se o modo de agente de instância única padrão estiver sendo usado.

Identificador: MQ_RABBIT_DEPLOYMENT_MODE

Tipos de recursos: AWS::AmazonMQ::Broker

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

msk-enhanced-monitoring-enabled

Verifica se o monitoramento aprimorado está habilitado para um cluster do Amazon MSK definido como PER_TOPIC_PER_BROKER ou PER_TOPIC_PER_PARTITION. A regra será NON_COMPLIANT se o monitoramento aprimorado estiver habilitado e definido como DEFAULT ou PER_BROKER.

Identificador: MSK_ENHANCED_MONITORING_ENABLED

Tipos de recursos: AWS::MSK::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

msk-in-cluster-node-require-tls

Verifica se um cluster do Amazon MSK impõe criptografia em trânsito usando HTTPS (TLS) com os nós de agente do cluster. A regra será NON_COMPLIANT se a comunicação de texto sem formatação estiver habilitada para conexões de nós do broker no cluster.

Identificador: MSK_IN_CLUSTER_NODE_REQUIRE_TLS

Tipos de recursos: AWS::MSK::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

multi-region-cloudtrail-enabled

> **Important**
>
> Para essa regra, o identificador da regra (MULTI_REGION_CLOUD_TRAIL_ENABLED) e o nome da regra (multi-region-cloudtrail-enabled) são diferentes.

Verifica se há pelo menos uma multirregião. AWS CloudTrail A regra será NON_COMPLIANT se as trilhas não corresponderem aos parâmetros de entrada. A regra é NON_COMPLIANT se

o `ExcludeManagementEventSources` campo não estiver vazio ou se AWS CloudTrail estiver configurado para excluir eventos de gerenciamento, como eventos AWS KMS ou eventos da API de dados do Amazon RDS.

Identifier (Identificador): MULTI_REGION_CLOUD_TRAIL_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

s3 BucketName (opcional), Tipo: string

Nome do bucket do Amazon S3 para o qual AWS CloudTrail entregar os arquivos de log.

snsTopicArn (Opcional), Tipo: string

ARN do tópico do Amazon SNS AWS CloudTrail para uso em notificações.

nuvem WatchLogsLogGroupArn (opcional), Tipo: string

ARN do grupo de CloudWatch registros da Amazon AWS CloudTrail para o qual enviar dados.

includeManagementEvents (Opcional), Tipo: booliano

Seletor de eventos para incluir eventos de gerenciamento para o. AWS CloudTrail

readWriteType (Opcional), Tipo: string

Tipo de eventos a serem registrados. Os valores válidos são ReadOnly, WriteOnly e ALL.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

nacl-no-unrestricted-ssh-rdp

Verifica se as portas padrão para tráfego de entrada SSH/RDP para listas de controle de acesso à rede (NACLs) são irrestritas. A regra será NON_COMPLIANT se uma entrada NACL permitir um bloco CIDR TCP ou UDP de origem para as portas 22 ou 3389.

Identificador: NACL_NO_UNRESTRICTED_SSH_RDP

Tipos de recursos: AWS::EC2::NetworkAcl

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-backup-retention-check

Verifica se um período de retenção do cluster de banco de dados do Amazon Neptune está definido para um número específico de dias. A regra será NON_COMPLIANT se o período de retenção for menor que o valor especificado pelo parâmetro.

Identificador: NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mínimo BackupRetentionPeriod (opcional), Tipo: int

> Os backups mínimos de dias devem ser mantidos. Valores válidos de 1 a 35, o valor padrão é 7. A regra é NON_COMPLIANT se o valor for maior que 'backup'. RetentionPeriod A regra é COMPATÍVEL se o valor for menor ou igual a 'backup'RetentionPeriod.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-cloudwatch-log-export-enabled

Verifica se um cluster do Amazon Neptune CloudWatch tem a exportação de registros habilitada para registros de auditoria. A regra é NON_COMPLIANT se um cluster do Neptune não tiver CloudWatch a exportação de registros habilitada para registros de auditoria.

Identificador: NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-copy-tags-to-snapshot-enabled

Verifica se um cluster do Amazon Neptune está configurado para copiar todas as tags para snapshots quando os snapshots são criados. A regra é NON_COMPLIANT se a opção “copiar TagsTo instantâneo” estiver definida como false.

Identificador: NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-deletion-protection-enabled

Verifica se um cluster de banco de dados do Amazon Neptune tem a proteção contra exclusão habilitada. A regra será NON_COMPLIANT se um cluster do Amazon Neptune tiver o campo deletionProtection definido como falso.

Identificador: NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-encrypted

Verifica se a criptografia de armazenamento está habilitada para seus clusters de banco de dados do Amazon Neptune. A regra será NON_COMPLIANT se a criptografia de armazenamento não estiver habilitada.

Identificador: NEPTUNE_CLUSTER_ENCRYPTED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

KmsKeyArns (Opcional), Tipo: Csv

Uma lista separada por vírgulas de ARNs de chaves KMS para comparar com a KmsKeyId do cluster criptografado.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-iam-database-authentication

Verifica se um cluster do Amazon Neptune AWS tem a autenticação de banco de dados Identity and Access Management (IAM) ativada. A regra é NON_COMPLIANT se um cluster do Amazon Neptune não tiver a autenticação de banco de dados do IAM habilitada.

Identificador: NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-multi-az-enabled

Verifica se um cluster do Amazon Neptune está configurado com a replicação multi-AZ do Amazon RDS. A regra será NON_COMPLIANT se a replicação multi-AZ não estiver habilitada.

Identificador: NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-snapshot-encrypted

Verifica se um cluster de banco de dados do Amazon Neptune tem snapshots criptografados. A regra será NON_COMPLIANT se um cluster do Neptune não tiver snapshots criptografados.

Identificador: NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

Tipos de recursos: AWS: :RDS: :DB ClusterSnapshot

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

neptune-cluster-snapshot-public-prohibited

Verifica se um snapshot manual do cluster de banco de dados do Amazon Neptune é público. A regra será NON_COMPLIANT se qualquer snapshot de cluster do Neptune novo e existente for público.

Identificador: NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

Tipos de recursos: AWS: :RDS: :DB ClusterSnapshot

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-deletion-protection-enabled

Verifica se o AWS Network Firewall tem a proteção contra exclusão ativada. A regra será NON_COMPLIANT se o Network Firewall não tiver a proteção contra exclusão habilitada.

Identificador: NETFW_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::NetworkFirewall::Firewall

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-logging-enabled

Verifica se os firewalls do AWS Network Firewall têm o registro ativado. A regra será NON_COMPLIANT se o tipo de registro em log não estiver configurado. Você pode especificar qual tipo de registro em log você deseja que a regra verifique.

Identificador: NETFW_LOGGING_ENABLED

Tipos de recursos: AWS::NetworkFirewall::LoggingConfiguration

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

logType (opcional), Tipo: string

LogType (opcional): tipo de log para verificação da regra de firewalls: 'alert', 'flow' ou 'both'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-multi-az-enabled

Verifica se os firewalls do AWS Network Firewall estão implantados em várias zonas de disponibilidade. A regra é NON_COMPLIANT se os firewalls forem implantados em apenas uma zona de disponibilidade ou em menos zonas do que o número listado no parâmetro opcional.

Identificador: NETFW_MULTI_AZ_ENABLED

Tipos de recursos: AWS::NetworkFirewall::Firewall

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

availabilityZones (opcional), Tipo: int

O número de zonas de disponibilidade esperadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-policy-default-action-fragment-packets

Verifica se uma política AWS de Firewall de Rede está configurada com uma ação padrão sem estado definida pelo usuário para pacotes fragmentados. A regra é NON_COMPLIANT se a ação padrão sem estado para pacotes fragmentados não corresponder à ação padrão definida pelo usuário.

Identificador: NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Ações apátridas FragmentDefault, Tipo: Csv

> Lista de valores separados por vírgula. Você pode selecionar no máximo dois. Os valores válidos incluem 'aws:pass', 'aws:drop' e 'aws:forward_to_sfe'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

netfw-policy-default-action-full-packets

Verifica se uma política AWS de Firewall de Rede está configurada com uma ação sem estado padrão definida pelo usuário para pacotes completos. Essa regra será NON_COMPLIANT se a ação sem estado padrão para pacotes completos não corresponder à ação sem estado padrão definida pelo usuário.

Identificador: NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

apátrida DefaultActions, Tipo: Csv

Lista de valores separados por vírgula. Você pode selecionar no máximo dois. Os valores válidos incluem 'aws:pass', 'aws:drop' e 'aws:forward_to_sfe'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-policy-rule-group-associated

Verifique se a política de Firewall de AWS Rede está associada a grupos de regras com ou sem estado. Essa regra será NON_COMPLIANT se nenhum grupo de regras stateful ou sem estado estiver associado à política de Firewall de Rede. Caso contrário, será COMPLIANT se algum dos grupos de regras existir.

Identificador: NETFW_POLICY_RULE_GROUP_ASSOCIATED

Tipos de recursos: AWS::NetworkFirewall::FirewallPolicy

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

netfw-stateless-rule-group-not-empty

Verifica se um grupo de regras sem estado do Network Firewall contém regras. A regra é NON_COMPLIANT se não houver regras em um grupo de regras sem estado do Network Firewall.

Identificador: NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

Tipos de recursos: AWS::NetworkFirewall::RuleGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

nlb-cross-zone-load-balancing-enabled

Verifica se o balanceamento de carga entre zonas está habilitado nos Network Load Balancers (NLBs). A regra é NON_COMPLIANT. se o balanceamento de carga entre zonas não estiver habilitado para um NLB.

Identificador: NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

Tipos de recursos: AWS::ElasticLoadBalancingV2::LoadBalancer

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

no-unrestricted-route-to-igw

Verifica se há rotas públicas na tabela de rotas para um gateway da Internet (IGW). A regra será NON_COMPLIANT se uma rota para um IGW tiver um bloco CIDR de destino '0.0.0.0/0' ou '::/0' ou se um bloco CIDR de destino não corresponder ao parâmetro da regra.

Identificador: NO_UNRESTRICTED_ROUTE_TO_IGW

Tipos de recursos: AWS::EC2::RouteTable

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

routeTableIds (Opcional), Tipo: Csv

> Lista separada por vírgulas de IDs de tabela de rotas que podem ter rotas para um Gateway da Internet com um bloco CIDR de destino de '0.0.0.0/0' ou '::/0'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-access-control-enabled

Verifica se os domínios OpenSearch do Amazon Service têm um controle de acesso refinado ativado. A regra é NON_COMPLIANT se não AdvancedSecurityOptions estiver habilitada para o OpenSearch domínio Service.

Identificador: OPENSEARCH_ACCESS_CONTROL_ENABLED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-audit-logging-enabled

Verifica se os domínios OpenSearch do Amazon Service têm o registro de auditoria ativado. A regra é NON_COMPLIANT se um domínio OpenSearch de serviço não tiver o registro de auditoria ativado.

Identificador: OPENSEARCH_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

nuvem WatchLogsLogGroupArnList (opcional), Tipo: Csv

> Lista separada por vírgula de nomes de recursos da Amazon (ARNs) para grupos de log do Amazon CloudWatch Logs. A regra verifica se os grupos de registros especificados estão configurados para registros de auditoria.
>
> Os valores válidos incluem: `arn:aws:logs:region:account-id:log-group:log_group_name:*` e `arn:aws:logs:region:account-id:log-group:log_group_name`.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

opensearch-data-node-fault-tolerance

Verifica se os domínios do Amazon OpenSearch Service estão configurados com pelo menos três nós de dados e zoneAwarenessEnabled se são verdadeiros. A regra é NON_COMPLIANT para um OpenSearch domínio se 'instanceCount' for menor que 3 ou 'zone' estiver definida como 'false'. AwarenessEnabled

Identificador: OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-encrypted-at-rest

Verifica se os domínios do Amazon OpenSearch Service têm a configuração de criptografia em repouso ativada. A regra será NON_COMPLIANT se o campo `EncryptionAtRestOptions` não estiver habilitado.

> **Note**
>
> A regra não avalia os domínios do Elasticsearch.

Identificador: OPENSEARCH_ENCRYPTED_AT_REST

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-https-required

Verifica se as conexões com OpenSearch domínios estão usando HTTPS. A regra é NON_COMPLIANT se o domínio da Amazon OpenSearch 'EnforceHTTPS' não for 'verdadeiro' ou for 'verdadeiro' e SecurityPolicy 'TLS 'não estiver em' '. `tlsPolicies`

Identificador: OPENSEARCH_HTTPS_REQUIRED

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

tlsPolicies (opcional), Tipo: Csv

> Lista separada por vírgulas de políticas de segurança de TLS a serem comparadas com o domínio da Amazon. OpensSearch

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

opensearch-in-vpc-only

Verifica se os domínios do Amazon OpenSearch Service estão em uma Amazon Virtual Private Cloud (VPC). A regra é NON_COMPLIANT se um endpoint de domínio OpenSearch de serviço for público.

> **Note**
>
> A regra não avalia os domínios do Elasticsearch.

Identificador: OPENSEARCH_IN_VPC_ONLY

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-logs-to-cloudwatch

Verifica se os domínios do Amazon OpenSearch Service estão configurados para enviar registros para o Amazon CloudWatch Logs. A regra será NON_COMPLIANT se o registro em log não estiver configurado.

> **Note**
>
> A regra não avalia os domínios do Elasticsearch.

Identificador: OPENSEARCH_LOGS_TO_CLOUDWATCH

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

logTypes (opcional), Tipo: Csv

Lista separada por vírgulas de logs que estão habilitados. Os valores válidos são 'search', 'index', 'error'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-node-to-node-encryption-check

Verifique se os nós do Amazon OpenSearch Service estão criptografados de ponta a ponta. A regra é NON_COMPLIANT se a node-to-node criptografia não estiver habilitada no domínio

> **Note**
>
> A regra não avalia os domínios do Elasticsearch.

Identificador: OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

opensearch-primary-node-fault-tolerance

Verifica se os domínios do Amazon OpenSearch Service estão configurados com pelo menos três nós primários dedicados. A regra é NON_COMPLIANT para um domínio OpenSearch de serviço se 'DedicatedMasterAtivado' estiver definido como 'falso' ou 'DedicatedMasterContagem' for menor que 3.

Identificador: OPENSEARCH_PRIMARY_NODE_FAULT_TOLERANCE

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

opensearch-update-check

Verifica se as atualizações OpenSearch de versão do Amazon Service estão disponíveis, mas não instaladas. A regra é NON_COMPLIANT para um OpenSearch domínio se as atualizações de software mais recentes não estiverem instaladas.

Identificador: OPENSEARCH_UPDATE_CHECK

Tipos de recursos: AWS::OpenSearch::Domain

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-aurora-mysql-audit-logging-enabled

Verifica se os clusters da edição compatível com o Amazon Aurora MySQL estão configurados para publicar logs de auditoria no Amazon Logs. CloudWatch A regra será NON_COMPLIANT se os clusters do Aurora MySQL-Compatible Edition não tiverem a publicação de logs de auditoria configurada.

Identificador: RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-automatic-minor-version-upgrade-enabled

Verifica se as instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS) estão configuradas para atualizações automáticas de versões secundárias. A regra é NON_COMPLIANT se o valor de “atualização automática” MinorVersion for falso.

Identificador: RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* Para obter mais informações sobre valores válidos para essas entradas, consulte AutoMinorVersionUpgrade o Engine no Guia do AWS CloudFormation Usuário.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-cluster-auto-minor-version-upgrade-enable

Verifica se as atualizações automáticas de versões secundárias estão habilitadas para implantações de cluster multi-AZ do Amazon RDS. A regra será NON_COMPLIANT se a autoMinorVersion atualização estiver definida como false.

Identificador: RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-cluster-default-admin-check

Verifica se um cluster de banco de dados do Amazon Relational Database Service (Amazon RDS) alterou o nome de usuário do administrador de seu valor padrão. A regra será NON_COMPLIANT se o nome de usuário do administrador estiver definido com o valor padrão.

Identificador: RDS_CLUSTER_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

válido AdminUserNames (opcional), Tipo: Csv

> Lista separada por vírgulas de nomes de usuários do administrador que os clusters do Amazon RDS podem usar. Não é possível incluir 'postgres' ou 'admin' como nomes de usuários válidos, pois esses são valores padrão.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

rds-cluster-deletion-protection-enabled

Verifica se um cluster do Amazon Relational Database Service (Amazon RDS) tem a proteção de exclusão habilitada. A regra será NON_COMPLIANT se um cluster do Amazon RDS não tiver a proteção de exclusão habilitada.

Identificador: RDS_CLUSTER_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-cluster-encrypted-at-rest

Verifica se um cluster do Amazon Relational Database Service (Amazon RDS) está criptografado em repouso. A regra será NON_COMPLIANT se um cluster do Amazon RDS não estiver criptografado em repouso.

Identificador: RDS_CLUSTER_ENCRYPTED_AT_REST

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-cluster-iam-authentication-enabled

Verifica se um cluster do Amazon Relational Database Service (Amazon RDS) AWS tem a autenticação Identity and Access Management (IAM) ativada. A regra será NON_COMPLIANT se um cluster do Amazon RDS não tiver a autenticação do IAM habilitada.

Identificador: RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-cluster-multi-az-enabled

Verifica se a replicação da zona de disponibilidade múltipla (multi-AZ) está habilitada nos clusters do Amazon Aurora e Hermes gerenciados pelo Amazon Relational Database Service (Amazon RDS). A regra é NON_COMPLIANT se uma instância do Amazon RDS não estiver configurada com multi-AZ.

Identificador: RDS_CLUSTER_MULTI_AZ_ENABLED

Tipos de recursos: AWS::RDS::DBCluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-db-security-group-not-allowed

Verifica se há algum grupo de segurança de banco de dados do Amazon Relational Database Service (Amazon RDS) que não seja o grupo de segurança de banco de dados padrão. A regra será NON_COMPLIANT se houver algum grupo de segurança de banco de dados que não seja o grupo de segurança de banco de dados padrão.

Identificador: RDS_DB_SECURITY_GROUP_NOT_ALLOWED

Tipos de recursos: AWS: :RDS: :DB SecurityGroup

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na Europa (Irlanda), América do Sul (São Paulo)´, Leste dos EUA (N. da Virgínia), Ásia-Pacífico (Tóquio), Oeste dos EUA (Oregon), Oeste dos EUA (Norte da Califórnia), Ásia-Pacífico (Singapura), Ásia-Pacífico (Sydney)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-enhanced-monitoring-enabled

Verifica se o monitoramento aprimorado está habilitado para instâncias do Amazon RDS. Essa regra é NON_COMPLIANT se '`monitoringInterval`' for '0' no item de configuração da instância do RDS ou se '`monitoringInterval`' não corresponder ao valor do parâmetro da regra.

Identifier (Identificador): RDS_ENHANCED_MONITORING_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

monitoringInterval (opcional), Tipo: int

> Um valor inteiro em segundos entre os pontos nos quais as métricas de monitoramento avançado são coletadas para a instância do banco de dados. Os valores válidos são 1, 5, 10, 15, 30 e 60.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o

esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* Para obter mais informações sobre valores válidos para essas entradas, consulte MonitoringIntervalo Engine no Guia do AWS CloudFormation Usuário.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-instance-default-admin-check

Verifica se o banco de dados do Amazon Relational Database Service (Amazon RDS) alterou o nome de usuário do administrador de seu valor padrão. Essa regra só será executada em instâncias de banco de dados do RDS. A regra será NON_COMPLIANT se o nome de usuário do administrador estiver definido com o valor padrão.

Identificador: RDS_INSTANCE_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

válido AdminUserNames (opcional), Tipo: Csv

> Lista separada por vírgulas de nomes de usuários do administrador que as instâncias do Amazon RDS podem usar. (Não é possível incluir 'postgres' ou 'admin' como nomes de usuários válidos, pois esses são valores padrão.)

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-instance-deletion-protection-enabled

Verifica se uma instância do Amazon Relational Database Service (Amazon RDS) tem a proteção de exclusão habilitada. A regra será NON_COMPLIANT se uma instância do Amazon RDS não tiver a proteção de exclusão habilitada; por exemplo, deletionProtection está definida como falsa.

> **Warning**
>
> Algumas instâncias de banco de dados do RDS em um cluster (Aurora/DocumentDB) aparecerão como não compatíveis.

Identificador: RDS_INSTANCE_DELETION_PROTECTION_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

databaseEngines (opcional), Tipo: Csv

Lista separada por vírgulas de mecanismos de banco de dados do RDS para incluir na avaliação da regra. Por exemplo, 'mysql, postgres, mariadb'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-instance-iam-authentication-enabled

Verifica se uma instância do Amazon Relational Database Service (Amazon RDS) AWS tem a autenticação Identity and Access Management (IAM) ativada. A regra será NON_COMPLIANT se uma instância do Amazon RDS não tiver a autenticação do IAM habilitada.

> **Note**
>
> O mecanismo de banco de dados deve ser 'mysql', 'postgres', 'aurora', 'aurora-mysql' ou 'aurora-postgresql'. O status da instância de banco de dados deve ser “disponível”, “backup”, “otimização de armazenamento” ou “armazenamento cheio”.

Identificador: RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

rds-instance-public-access-check

Verifica se instâncias do Amazon Relational Database Service (Amazon RDS) não estão acessíveis ao público. Essa regra será NON_COMPLIANT se o campo publiclyAccessible for verdadeiro no item de configuração da instância.

Identifier (Identificador): RDS_INSTANCE_PUBLIC_ACCESS_CHECK

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-in-backup-plan

Verifica se os bancos de dados do Amazon Relational Database Service (Amazon RDS) estão presentes nos planos de AWS Backup. A regra é NON_COMPLIANT se os bancos de dados do Amazon RDS não estiverem incluídos em nenhum plano de Backup. AWS

> **Note**
>
> A regra é aplicável somente a instâncias de banco de dados do Amazon Aurora. Não há suporte para os clusters de banco de dados.

Identificador: RDS_IN_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para o Amazon Relational Database Service (Amazon RDS). A regra será NON_COMPLIANT se a instância do Amazon RDS não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::RDS::DBInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags de instâncias do Amazon RDS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID da instância do Amazon RDS para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-logging-enabled

Verifica se os respectivos logs do Amazon Relational Database Service (Amazon RDS) estão habilitados. A regra será NON_COMPLIANT se os tipos de log não estiverem habilitados.

> **Note**
>
> As instâncias de banco de dados que não estão no status “disponível”, “backup”, “otimização de armazenamento” ou “armazenamento cheio” são avaliadas como `NOT_APPLICABLE`.

Identificador: RDS_LOGGING_ENABLED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

additionalLogs (opcional), Tipo: StringMap

Lista separada por vírgulas de nomes do mecanismo e nomes do tipo de log. Por exemplo, “additionalLogs”: “oracle: general, slowquery; aurora: alert, slowquery”

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-meets-restore-time-target

Confere se o tempo de restauração das instâncias do Amazon Relational Database Service (Amazon RDS) atende à duração especificada. A regra é NON_COMPLIANT se LatestRestoreExecutionTimeMinutes uma instância do Amazon RDS for maior que minutos. maxRestoreTime

Identificador: RDS_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::RDS::DBInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags de instâncias do Amazon RDS para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID da instância do Amazon RDS para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-multi-az-support

Verifica se a alta disponibilidade está ativada para suas instâncias de banco de dados do RDS.

Em uma implantação Multi-AZ, o Amazon RDS automaticamente provisiona e mantém uma réplica em espera síncrona em outra Zona de disponibilidade. Para mais informações, consulte High Availability (multi-AZ) no Guia do usuário do Amazon RDS.

> **Note**
>
> Essa regra não avalia as instâncias de banco de dados do Amazon Aurora, do Amazon DocumentDB e do Amazon Neptune.

Identifier (Identificador): RDS_MULTI_AZ_SUPPORT

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* Para obter mais informações sobre valores válidos para essas entradas, consulte MultiAZ e Engine no Guia AWS CloudFormation do Usuário.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-resources-protected-by-backup-plan

Verifica se instâncias do Amazon Relational Database Service (Amazon RDS) estão protegidas por um plano de backup. A regra será NON_COMPLIANT se a instância do banco de dados do Amazon RDS não estiver coberta por um plano de backup.

Identificador: RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::RDS::DBInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para instâncias do Amazon RDS para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID da instância do Amazon RDS para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-snapshots-public-prohibited

Verifica se os snapshots do Amazon Relational Database Service (Amazon RDS) são públicos. A regra será NON_COMPLIANT se os snapshots novos e existentes do Amazon RDS forem públicos.

> **Note**
>
> A captura de resultados de conformidade pode levar até 12 horas.

Identifier (Identificador): RDS_SNAPSHOTS_PUBLIC_PROHIBITED

Tipos de recursos: AWS: :RDS: :DBSnapshot, AWS: :RDS: :DB ClusterSnapshot

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-snapshot-encrypted

Verifica se os snapshots do banco de dados do Amazon Relational Database Service (Amazon RDS) são criptografados. A regra será NON_COMPLIANT se os snapshots de banco de dados do Amazon RDS não forem criptografados.

Identificador: RDS_SNAPSHOT_ENCRYPTED

Tipos de recursos: AWS: :RDS: :DBSnapshot, AWS: :RDS: :DB ClusterSnapshot

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

rds-storage-encrypted

Verifica se a criptografia de armazenamento está habilitada para instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS). A regra será NON_COMPLIANT se a criptografia de armazenamento não estiver habilitada.

Identifier (Identificador): RDS_STORAGE_ENCRYPTED

Tipos de recursos: AWS::RDS::DBInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyId (Opcional), Tipo: string

> ID de chave do KMS ou nome do recurso da Amazon (ARN) usado para criptografar o armazenamento.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-audit-logging-enabled

Verifica se os clusters do Amazon Redshift estão registrando auditorias em um bucket específico. A regra será NON_COMPLIANT se o registro em log de auditoria não estiver habilitado para um cluster do Redshift ou se o parâmetro '`bucketNames`' for fornecido, mas o destino do registro em log de auditoria não for correspondente.

Identificador: REDSHIFT_AUDIT_LOGGING_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

bucketNames (opcional), Tipo: Csv

> Lista separada por vírgulas dos nomes de buckets do Amazon S3 para armazenar logs de auditoria.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-backup-enabled

Verifica se os snapshots automatizados do Amazon Redshift estão habilitados para clusters. A regra será NON_COMPLIANT se o valor `automatedSnapshotRetentionPeriod` for maior que `MaxRetentionPeriod` ou menor que `MinRetentionPeriod` ou se o valor for 0.

Identificador: REDSHIFT_BACKUP_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

MinRetentionPeriod (Opcional), Tipo: int

Valor mínimo do período de retenção. O valor mínimo é 1.

MaxRetentionPeriod (Opcional), Tipo: int

Valor máximo do período de retenção. O valor máximo é 35.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-cluster-configuration-check

Verifica se os clusters do Amazon Redshift têm as configurações especificadas. A regra será NON_COMPLIANT se o cluster do Amazon Redshift não estiver criptografado ou criptografado com outra chave, ou se um cluster não tiver o registro em log de auditoria habilitado.

Identifier (Identificador): REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

agrupamento DbEncrypted, Tipo: booliano, Padrão: True

A criptografia de banco de dados está habilitada.

loggingEnabled, Tipo: booliano, Padrão: True

O log de auditoria está habilitado.

nodeTypes (opcional), Tipo: Csv, Padrão: dc1.large

Especifica o tipo de nó.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-cluster-kms-enabled

Verifica se os clusters do Amazon Redshift estão usando uma chave especificada AWS Key Management Service (AWS KMS) para criptografia. A regra será COMPLIANT se a criptografia estiver habilitada e o cluster for criptografado com a chave fornecida no parâmetro `kmsKeyArn`. A regra será NON_COMPLIANT se o cluster não estiver criptografado ou foi criptografado com outra chave.

Identificador: REDSHIFT_CLUSTER_KMS_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

Lista separada por vírgula dos principais nomes de recursos da AWS KMS Amazon (ARNs) usados nos clusters do Amazon Redshift para criptografia.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-cluster-maintenancesettings-check

Verifica se os clusters do Amazon Redshift têm as configurações de manutenção especificadas. A regra será NON_COMPLIANT se as atualizações automáticas para a versão principal estiverem desabilitadas.

Identifier (Identificador): REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

permitir VersionUpgrade, Tipo: booliano, Padrão: True

Permitir atualização de versão está ativado.

preferredMaintenanceWindow (Opcional), Tipo: string

A janela de manutenção programada para clusters (por exemplo, Seg:09:30-Seg:10:00).

automatizado SnapshotRetentionPeriod (opcional), Tipo: int, Padrão: 1

Número de dias para reter snapshots automatizados.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* Para obter mais informações sobre valores válidos para essas entradas AutomatedSnapshotRetentionPeriod, consulte PreferredMaintenanceJanela e AllowVersionatualização no Guia do AWS CloudFormation usuário.

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-cluster-public-access-check

Verifica se os clusters do Amazon Redshift não estão acessíveis publicamente. Essa regra será NON_COMPLIANT se o campo publiclyAccessible for verdadeiro no item de configuração do cluster.

Identifier (Identificador): REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift-default-admin-check

Verifica se um cluster do Amazon Redshift alterou o nome de usuário do administrador em relação ao valor padrão. A regra será NON_COMPLIANT se o nome de usuário do administrador de um cluster do Redshift estiver definido como “awsuser” ou se o nome de usuário não corresponder ao que está listado no parâmetro.

Identificador: REDSHIFT_DEFAULT_ADMIN_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

válido AdminUserNames (opcional), Tipo: Csv

> Lista separada por vírgulas de nomes de usuários do administrador para uso pelos clusters do Redshift. Observação: 'awsuser' é o padrão e não é aceito.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

redshift-default-db-name-check

Verifica se um cluster do Redshift mudou o nome do banco de dados em relação ao valor padrão. A regra será NON_COMPLIANT se o nome do banco de dados de um cluster do Redshift estiver definido como “dev” ou se o parâmetro opcional for fornecido e o nome do banco de dados não for correspondente.

Identificador: REDSHIFT_DEFAULT_DB_NAME_CHECK

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

validDatabaseNames (Opcional), Tipo: Csv

Lista separada por vírgulas de nomes de bancos de dados para clusters do Redshift.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

redshift-enhanced-vpc-routing-enabled

Verifica se o cluster do Amazon Redshift tem a opção “aprimorada” ativadaVpcRouting. A regra é NON_COMPLIANT se a opção VpcRouting 'aprimorada' não estiver habilitada ou se a configuração. enhancedVpcRouting o campo é 'falso'.

Identificador: REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

Tipos de recursos: AWS::Redshift::Cluster

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

redshift-require-tls-ssl

Verifica se os clusters do Amazon Redshift exigem criptografia TLS/SSL para se conectar a clientes SQL. A regra será NON_COMPLIANT se qualquer cluster do Amazon Redshift tiver o parâmetro require_SSL não definido como verdadeiro.

Identificador: REDSHIFT_REQUIRE_TLS_SSL

Tipos de recursos: AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter Grupo

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

redshift - acesso irrestrito à porta

Verifica se os grupos de segurança associados a um cluster do Amazon Redshift têm regras de entrada que permitem tráfego de entrada irrestrito. A regra é NON_COMPLIANT se houver regras de entrada que permitam tráfego de entrada irrestrito para a porta de cluster do Redshift.

Identificador: REDSHIFT_UNRESTRICTED_PORT_ACCESS

Tipos de recursos: AWS::Redshift::Cluster

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

required-tags

Verifica se seus recursos têm as tags que você especificou. Por exemplo, você pode verificar se suas instâncias do Amazon EC2 têm a tag `CostCenter`, além de verificar se todas as suas

instâncias do RDS têm um conjunto de tags de Chaves. Separe com vírgulas os vários valores. Você pode verificar até seis tags por vez.

O documento AWS de AWS Systems Manager automação gerenciada `AWS-SetRequiredTags` não funciona como uma remediação com essa regra. Você precisará criar sua própria documentação personalizada de automação do Systems Manager para correção.

Contexto: AWS permite atribuir metadados aos AWS recursos na forma de tags. Cada tag é um rótulo que consiste em uma chave e um valor opcional para armazenar informações sobre o recurso ou os dados retidos nesse recurso. Para obter mais informações, consulte Building your tagging strategy.

Você pode usar essa regra para encontrar recursos em sua conta que não foram lançados com as configurações desejadas especificando quais recursos devem ter tags e o valor esperado para cada tag. Você também pode executar ações de correção para corrigir erros de marcação. No entanto, essa regra não impede que você crie recursos com tags incorretas.

Identifier (Identificador): REQUIRED_TAGS

Tipos de recursos AWS::ACM::Certificate, AWS::AutoScaling::: AutoScaling Grupo, AWS::CloudFormation::Stack, AWS::CodeBuild: :Projeto AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable, AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoad Balanceamento:: LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription,, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter AWS::Redshift::ClusterSecurity Grupo, Grupo AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnet AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

tag1Key, Tipo: string, Padrão: CostCenter

Chave da tag necessária.

tag1Value (opcional), Tipo: Csv

Valor opcional da tag necessária. Separe com vírgulas os vários valores.

tag2Key (opcional), Tipo: string

Chave de uma segunda etiqueta obrigatória.

tag2Value (opcional), Tipo: Csv

Valor opcional da segunda tag obrigatória. Separe com vírgulas os vários valores.

tag3Key (opcional), Tipo: string

Chave de uma terceira tag obrigatória.

tag3Value (opcional), Tipo: Csv

Valor opcional da terceira tag obrigatória. Separe com vírgulas os vários valores.

tag4Key (opcional), Tipo: string

Chave de uma quarta etiqueta obrigatória.

tag4Value (opcional), Tipo: Csv

Valor opcional da quarta tag obrigatória. Separe com vírgulas os vários valores.

tag5Key (opcional), Tipo: string

Chave de uma quinta etiqueta obrigatória.

tag5Value (opcional), Tipo: Csv

Valor opcional da quinta tag obrigatória. Separe com vírgulas os vários valores.

tag6Key (opcional), Tipo: string

Chave de uma sexta etiqueta obrigatória.

tag6Value (opcional), Tipo: Csv

Valor opcional da sexta tag obrigatória. Separe com vírgulas os vários valores.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

restricted-common-ports

> **Important**
>
> Para essa regra, o identificador da regra (RESTRICTED_INCOMING_TRAFFIC) e o nome da regra (restricted-common-ports) são diferentes.

Verifica se os grupos de segurança em uso não permitem o tráfego de entrada do Transmission Control Protocol (TCP) irrestrito para as portas especificadas. A regra é COMPLIANT se:

- O acesso à porta está bloqueado para todo o tráfego TCP.
- O acesso à porta está aberto ao tráfego TCP por meio de regras de entrada, em que a origem é um único endereço IPv4 ou um intervalo de endereços IPv4 na notação CIDR que não abrange todos os endereços IPv4 ("0.0.0.0/0").
- O acesso à porta está aberto ao tráfego TCP por meio de regras de entrada, em que a origem é um único endereço IPv6 ou um intervalo de endereços IPv6 na notação CIDR que não abrange todos os endereços IPv6 (“::/0)”).

A regra será NON_COMPLIANT se os endereços IP das conexões TCP de entrada não estiverem restritos às portas especificadas.

Identifier (Identificador): RESTRICTED_INCOMING_TRAFFIC

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

blockedPort1 (opcional), Tipo: int, Padrão: 20

Número da porta TCP bloqueado. O padrão de 20 corresponde à transferência de dados do Protocolo de Transferência de Arquivos (FTP).

blockedPort2 (opcional), Tipo: int, Padrão: 21

Número da porta TCP bloqueado. O padrão de 21 corresponde ao controle de comando do Protocolo de Transferência de Arquivos (FTP).

blockedPort3 (opcional), Tipo: int, Padrão: 3389

Número da porta TCP bloqueado. O padrão de 3389 corresponde ao Protocolo RDP.

blockedPort4 (opcional), Tipo: int, Padrão: 3306

Número da porta TCP bloqueado. O padrão de 3306 corresponde ao protocolo MySQL.

blockedPort5 (opcional), Tipo: int, Padrão: 4333

Número da porta TCP bloqueado. O padrão de 4333 corresponde ao protocolo MySQL.

blockedPorts (opcional), Tipo: Csv

Lista separada por vírgulas de números de portas TCP bloqueadas. Por exemplo, 20, 21, 3306, 3389 e 4333.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

root-account-hardware-mfa-enabled

Verifica se sua AWS conta está habilitada para usar um dispositivo de hardware de autenticação multifator (MFA) para fazer login com credenciais raiz. A regra será NON_COMPLIANT se dispositivos MFA virtuais tiverem permissão para fazer login com as credenciais raiz.

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
> Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

root-account-mfa-enabled

Verifica se o usuário raiz da sua AWS conta exige autenticação multifator para fazer login no console. A regra é NON_COMPLIANT se o usuário da conta raiz do AWS Identity and Access Management (IAM) não tiver a autenticação multifator (MFA) ativada.

> **Note**
>
> Regras gerenciadas e tipos de recursos globais do IAM
> Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.
> Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você

não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.
Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Identifier (Identificador): ROOT_ACCOUNT_MFA_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

route53-query-logging-enabled

Verifica se o registro em log de consultas ao DNS está habilitado para suas zonas hospedadas públicas do Amazon Route 53. A regra será NON_COMPLIANT se o registro em log de consultas ao DNS não estiver habilitado para suas zonas hospedadas públicas do Amazon Route 53.

Identificador: ROUTE53_QUERY_LOGGING_ENABLED

Tipos de recursos: AWS::Route53::HostedZone

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-access-point-in-vpc-only

Verifica se um ponto de acesso do Amazon S3 não permite acesso pela Internet (é NetworkOrigin VPC). A regra é NON_COMPLIANT se for NetworkOrigin Internet.

Identificador: S3_ACCESS_POINT_IN_VPC_ONLY

Tipos de recursos: AWS::S3::AccessPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-access-point-public-access-blocks

Verifica se os pontos de acesso Amazon S3 têm configurações do bloqueio do acesso público habilitadas. A regra será NON_COMPLIANT se as configurações de bloqueio de acesso público não estiverem habilitadas para pontos de acesso S3.

Identificador: S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

Tipos de recursos: AWS::S3::AccessPoint

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

excludedAccessPoints (Opcional), Tipo: Csv

Lista de nomes separados por vírgula para pontos de acesso Amazon S3 públicos permitidos.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-account-level-public-access-blocks

Verifica se as configurações de bloco de acesso público necessárias estão configuradas no nível da conta. A regra será somente NON_COMPLIANT quando não houver a correspondência dos campos definidos abaixo com os campos correspondentes no item de configuração.

> **Note**
>
> Se você estiver usando essa regra, garanta que o S3 Block Public Access esteja habilitado. A regra é acionada por alterações, portanto, não será invocada a menos que o S3 Block Public Access esteja habilitado. Se o S3 Block Public Access não estiver habilitado, a regra retornará INSUFFICIENT_DATA. Isso significa que você ainda pode ter alguns buckets públicos. Para obter mais informações sobre como configurar o S3 Block Public Access, consulte Bloquear o acesso público ao armazenamento do Amazon S3.

Identifier (Identificador): S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

Tipos de recursos: AWS::S3::AccountPublic AccessBlock

Tipo de trigger: alterações de configuração (status atual não verificado, avaliado somente quando as alterações geram novos eventos)

> **Note**
>
> Essa regra só é acionada por alterações na configuração da região específica em que o endpoint do S3 está localizado. Em todas as outras regiões, a regra é verificada periodicamente. Se uma alteração foi feita em outra região, pode haver um atraso até que a regra retorne NON_COMPLIANT.

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

IgnorePublicAcls (Opcional), Tipo: string, Padrão: verdadeiro

IgnorePublicAcls é obrigatório ou não, padrão True

BlockPublicPolicy (Opcional), Tipo: string, Padrão: verdadeiro

BlockPublicPolicy é obrigatório ou não, padrão True

BlockPublicAcls (Opcional), Tipo: string, Padrão: verdadeiro

BlockPublicAcls é obrigatório ou não, padrão True

RestrictPublicBuckets (Opcional), Tipo: string, Padrão: verdadeiro

RestrictPublicBuckets é obrigatório ou não, padrão True

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-account-level-public-access-blocks-periodic

Verifica se as configurações de bloco de acesso público necessárias estão configuradas no nível da conta. A regra será NON_COMPLIANT se o item de configuração não corresponder a uma ou mais configurações dos parâmetros (ou padrão).

Identificador: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

IgnorePublicAcls (Opcional), Tipo: string

IgnorePublicAcls é obrigatório ou não, padrão True

BlockPublicPolicy (Opcional), Tipo: string

BlockPublicPolicy é obrigatório ou não, padrão True

BlockPublicAcls (Opcional), Tipo: string

BlockPublicAcls é obrigatório ou não, padrão True

RestrictPublicBuckets (Opcional), Tipo: string

RestrictPublicBuckets é obrigatório ou não, padrão True

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-acl-prohibited

Verifica se os buckets do Amazon Simple Storage Service (Amazon S3) concedem permissões de usuário por meio de listas de controle de acesso (ACLs). A regra será NON_COMPLIANT se as ACLs estiverem configuradas para acesso do usuário nos buckets do Amazon S3.

Identificador: S3_BUCKET_ACL_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-blacklisted-actions-prohibited

Verifica se uma política de bucket do Amazon Simple Storage Service (Amazon S3) não permite ações bloqueadas em nível de bucket e em nível de objeto em recursos no bucket para diretores de

outras contas. AWS Por exemplo, a regra verifica se a política de bucket do Amazon S3 não permite que outra AWS conta execute nenhuma `s3:GetBucket*` ação e `s3:DeleteObject` em nenhum objeto no bucket. A regra será NON_COMPLIANT se as ações que estiverem na lista de proibições forem permitidas pela política de buckets do Amazon S3.

> **Note**
>
> A regra verificará apenas entidades na propriedade da entidade principal e não levará em consideração quaisquer condicionais da propriedade Condição em uma política

Identifier (Identificador): S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

na lista negra ActionPattern, Tipo: Csv

Lista separada por vírgulas de padrões de ação na lista negra, por exemplo, s3: GetBucket * e s3:. DeleteObject

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

habilitado para replicação entre regiões de buckets s3

Verifica se você habilitou a replicação entre regiões do S3 para seus buckets do Amazon S3. A regra é NON_COMPLIANT se não houver regras de replicação habilitadas para replicação entre regiões.

Identificador: S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-default-lock-enabled

Verifica se o bucket do S3 tem o bloqueio habilitado, por padrão. A regra será NON_COMPLIANT se o bloqueio não estiver habilitado.

Identificador: S3_BUCKET_DEFAULT_LOCK_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

mode (opcional), Tipo: string

> modo: (opcional): um parâmetro de modo com valores válidos de GOVERNANCE ou COMPLIANCE.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-level-public-access-prohibited

Verifica se os buckets do S3 estão acessíveis ao público. A regra será NON_COMPLIANT se um bucket do S3 não estiver listado no parâmetro `excludedPublicBuckets` e as configurações no nível do bucket forem públicas.

Identificador: S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

excludedPublicBuckets (Opcional), Tipo: Csv

Lista separada por vírgulas de nomes conhecidos de buckets públicos permitidos do Amazon S3.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-logging-enabled

Verifica se o registro em log está habilitado para seus buckets do S3. A regra será NON_COMPLIANT se o registro em log não estiver habilitado.

Identifier (Identificador): S3_BUCKET_LOGGING_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

targetBucket (opcional), Tipo: string

Bucket do S3 de destino para armazenar os logs de acesso ao servidor.

targetPrefix (opcional), Tipo: string

Prefixo do bucket do S3 para armazenar os logs de acesso ao servidor.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "BucketName": "my-bucket",
   "LoggingConfiguration": {
         "DestinationBucketName": "my-log-bucket",
         "LogFilePrefix":"my-log"
   }
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-mfa-delete-enabled

Verifica se a Exclusão de MFA está habilitada na configuração do versionamento do bucket do Amazon Simple Storage Service (Amazon S3). A regra será NON_COMPLIANT se o Exclusão de MFA não estiver habilitada.

Identificador: S3_BUCKET_MFA_DELETE_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-policy-grantee-check

Verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, principais de serviços, endereços IP ou VPCs que você fornece. A regra será COMPLIANT se uma política de bucket não estiver presente.

Por exemplo, se o parâmetro de entrada para a regra for a lista de duas entidades principais: `111122223333` e `444455556666` e a política de bucket especificar que apenas `111122223333` pode acessar o bucket, a regra será COMPLIANT. Com os mesmos parâmetros de entrada: se a política de bucket especificar que `111122223333` e `444455556666` podem acessar o bucket, ela também será compatível. No entanto, se a política de bucket especificar que `999900009999` pode acessar o bucket, a regra será NON-COMPLIANT.

> **Note**
>
> Se uma política de bucket contiver mais de uma instrução, cada instrução na política de bucket será avaliada de acordo com essa regra.

Identifier (Identificador): S3_BUCKET_POLICY_GRANTEE_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

awsPrincipals (opcional), Tipo: Csv

> Lista separada por vírgulas de principais, como ARNs de usuário do IAM, ARNs de função do IAM e AWS contas, por exemplo, 'arn:aws:iam: :111122223333:user/alice, arn:aws:iam: :444455556666:role/bob, 123456789012'.

servicePrincipals (opcional), Tipo: Csv

Lista separada por vírgulas das entidades principais de serviços, por exemplo, 'cloudtrail.amazonaws.com, lambda.amazonaws.com'.

federatedUsers (opcional), Tipo: Csv

Lista separada por vírgulas de provedores de identidade para a federação de identidades da web, como Amazon Cognito e provedores de identidade SAML. Por exemplo, 'cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider'.

ipAddresses (opcional), Tipo: Csv

Lista separada por vírgulas de endereços IP formatados com CIDR, por exemplo, '10.0.0.1, 192.168.1.0/24, 2001:db8::/32'.

vpcIds (opcional), Tipo: Csv

Lista separada por vírgulas de IDs do Amazon Virtual Private Clouds (Amazon VPC), por exemplo, 'vpc-1234abc0, vpc-ab1234c0'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-policy-not-more-permissive

Verifica se as políticas de bucket do Amazon Simple Storage Service não autorizam outras permissões entre contas que controlem a política de bucket do Amazon S3 que você fornece.

> **Note**
>
> Se você fornecer um valor de parâmetro inválido, verá o seguinte erro: O valor para o parâmetro controlPolicy deve ser uma política de buckets do Amazon S3.

Identifier (Identificador): S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

controlPolicy, Tipo: string

A política de bucket do Amazon S3 que define um limite máximo das permissões de seus buckets do S3. A política pode ter, no máximo, 1.024 caracteres.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-public-read-prohibited

Verifica se seus buckets do Amazon S3 permitem acesso público de leitura. A regra verifica o as configurações do Block Public Access, a política do bucket e a lista de controle de acesso (ACL) do bucket.

A regra é compatível quando estas duas condições são verdadeiras:

- A configuração do Block Public Access restringe as políticas públicas ou a política do bucket não permite acesso público de leitura.
- A configuração do Block Public Access restringe ACLs públicas ou a ACL do bucket não permite acesso público de leitura.

A regra não está em conformidade:

- Se a configuração Bloquear acesso público não restringir as políticas públicas, AWS Config avalia se a política permite acesso público de leitura. Se a política permitir acesso público de leitura, a regra não estará em conformidade.
- Se a configuração Bloquear acesso público não restringir ACLs de bucket público, AWS Config avalia se a ACL de bucket permite acesso público de leitura. Se a ACL do bucket permitir acesso público de leitura, a regra não estará em conformidade.

Identifier (Identificador): S3_BUCKET_PUBLIC_READ_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-public-write-prohibited

Verifica se seus buckets do Amazon S3 permitem acesso público de gravação. A regra verifica o as configurações do Block Public Access, a política do bucket e a lista de controle de acesso (ACL) do bucket.

A regra é compatível quando estas duas condições são verdadeiras:

- A configuração do Block Public Access restringe as políticas públicas ou a política do bucket não permite acesso público de gravação.
- A configuração do Block Public Access restringe ACLs públicas ou a ACL do bucket não permite acesso público de gravação.

A regra não está em conformidade:

- Se a configuração Bloquear acesso público não restringir as políticas públicas, AWS Config avalia se a política permite acesso público de gravação. Se a política permitir acesso público de gravação, a regra não estará em conformidade.
- Se a configuração Bloquear acesso público não restringir ACLs de bucket público, AWS Config avalia se a ACL de bucket permite acesso público de gravação. Se a ACL do bucket permitir acesso público de gravação, a regra não estará em conformidade.

> **Note**
>
> Essa regra não avalia as alterações no acesso ao bloco público no nível da conta. Para verificar se as configurações de bloqueio de acesso público necessárias estão definidas no

nível da conta, consulte s3-account-level-public-access-blocks e s3-account-level-public-access-blocks-periodic.

Identifier (Identificador): S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-replication-enabled

Verifica se os buckets do S3 têm regras de replicação habilitadas. A regra será NON_COMPLIANT se um bucket do S3 não tiver uma regra de replicação ou tiver uma regra de replicação que não esteja habilitada.

Identifier (Identificador): S3_BUCKET_REPLICATION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

ReplicationType (Opcional), Tipo: string

Valores aceitos: 'CROSS-REGION' e 'SAME-REGION'. Insira “CROSS-REGION” para a regra verificar se todos os buckets têm somente a replicação entre regiões habilitada. Insira “SAME-

REGION” para a regra verificar se todos os buckets têm somente a replicação na mesma região habilitada.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-server-side-encryption-enabled

Verifica se o bucket do Amazon S3 apresenta a criptografia padrão do Amazon S3 habilitada ou se a política de bucket do Amazon S3 nega explicitamente solicitações do `put-object`, sem criptografia do lado do servidor, que usa AES-256 ou AWS Key Management Service. A regra é NON_COMPLIANT se seu bucket do Amazon S3 não estiver criptografado por padrão.

Identifier (Identificador): S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-ssl-requests-only

Verifica se os buckets do S3 têm políticas que exigem solicitações para usar SSL/TLS. A regra será NON_COMPLIANT se algum bucket do S3 tiver políticas que permitam solicitações HTTP.

Identifier: S3_BUCKET_SSL_REQUESTS_ONLY

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-bucket-versioning-enabled

Verifica se o versionamento está habilitado para seus buckets do S3. Opcionalmente, a regra verifica se a exclusão MFA está habilitada para seus buckets do S3.

Identifier (Identificador): S3_BUCKET_VERSIONING_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

é MfaDeleteEnabled (opcional), Tipo: string

Exclusão MFA está habilitada para seus buckets do S3.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-default-encryption-kms

Verifica se os buckets do S3 estão criptografados com o AWS Key Management Service (AWS KMS). A regra é NON_COMPLIANT se o bucket do S3 não estiver criptografado com uma chave KMS. AWS

Identificador: S3_DEFAULT_ENCRYPTION_KMS

Tipos de recursos: AWS::S3::Bucket, AWS::KMS::Key

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

Lista separada por vírgula de ARNs de chave AWS KMS permitida para criptografar buckets do Amazon S3.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

s3-event-notifications-enabled

Verifica se notificações de eventos do Amazon S3 estão habilitadas em um bucket do S3. A regra será NON_COMPLIANT se as notificações de eventos do S3 não estiverem definidas em um bucket ou se o tipo ou o destino do evento não corresponderem aos parâmetros `eventTypes` e destinationArn.

Identificador: S3_EVENT_NOTIFICATIONS_ENABLED

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

destinationArn (opcional), Tipo: string

O Amazon Resource Name (ARN) do destino para a notificação do evento (tópico do Amazon SNS, AWS Lambda, Amazon SQS Queue).

eventTypes (opcional), Tipo: Csv

Lista separada por vírgulas dos tipos de eventos preferidos do Amazon S3

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para o Amazon Simple Storage Service (Amazon S3). A regra será NON_COMPLIANT se o bucket do Amazon S3 não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: S3_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::S3::Bucket

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags do bucket do Amazon S3 para a regra verificar, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

O nome do bucket do Amazon S3 para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-lifecycle-policy-check

Verifica se uma regra de ciclo de vida está configurada para um bucket do Amazon Simple Storage Service (Amazon S3). A regra será NON_COMPLIANT se não houver regras de configuração de ciclo de vida ativas ou se a configuração não corresponder aos valores dos parâmetros.

Identificador: S3_LIFECYCLE_POLICY_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

targetTransitionDays (Opcional), Tipo: int

Indica o número de dias após a criação do objeto em que os objetos farão a transição para a classe de armazenamento especificada (por exemplo, 30 dias).

targetExpirationDays (Opcional), Tipo: int

Número de dias após a criação do objeto quando os objetos são excluídos (por exemplo, 395 dias).

alvo TransitionStorageClass (opcional), Tipo: string

Tipo de classe de armazenamento de destino (por exemplo, Amazon S3 Standard-Infrequent Access (S3 Standard-IA). Para obter mais informações, consulte https: //docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html.

targetPrefix (opcional), Tipo: string

Prefixo de objeto do Amazon S3 para identificar um ou mais objetos.

bucketNames (opcional), Tipo: Csv

Lista separada por vírgulas de nomes de bucket do Amazon S3 que têm a política de ciclo de vida habilitada.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-meets-restore-time-target

Confere se o tempo de restauração dos buckets do Amazon Simple Storage Service (Amazon S3) atende à duração especificada. A regra é NON_COMPLIANT se um bucket LatestRestoreExecutionTimeMinutes do Amazon S3 for maior que minutos. maxRestoreTime

Identificador: S3_MEETS_RESTORE_TIME_TARGET

Tipos de recursos: AWS::S3::Bucket

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo RestoreTime, Tipo: int

Valor numérico do runtime máximo de restauração permitido.

resourceTags (opcional), Tipo: string

Tags do bucket do Amazon S3 para a regra verificar, no formato JSON .

resourceId (opcional), Tipo: string

O nome do bucket do Amazon S3 para verificação da regra.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

s3-resources-protected-by-backup-plan

Verifica se os buckets do Amazon Simple Storage Service (Amazon S3) estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o bucket do Amazon S3 não estiver coberto por um plano de backup.

Identificador: S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::S3::Bucket

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para buckets do Amazon S3 para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

O nome do bucket do Amazon S3 para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

s3-version-lifecycle-policy-check

Verifica se os buckets habilitados para a versão do Amazon Simple Storage Service (Amazon S3) têm a política de ciclo de vida configurada. A regra será NON_COMPLIANT se a política de ciclo de vida do Amazon S3 não estiver habilitada.

Identificador: S3_VERSION_LIFECYCLE_POLICY_CHECK

Tipos de recursos: AWS::S3::Bucket

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

bucketNames (opcional), Tipo: Csv

Lista separada por vírgulas de nomes de bucket do Amazon S3 que têm a política de ciclo de vida habilitada.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sagemaker-endpoint-configuration-kms-key-configured

Verifica se a AWS chave do Key Management Service (AWS KMS) está configurada para uma configuração de SageMaker endpoint da Amazon. A regra é NON_COMPLIANT se 'KmsKeyId' não for especificado para a configuração do endpoint da Amazon. SageMaker

Identifier (Identificador): SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

Tipos de recursos: AWS::SageMaker::EndpointConfig

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: string

Lista separada por vírgula de ARNs de chave AWS KMS específicos permitidos para uma configuração de endpoint da Amazon. SageMaker

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sagemaker-endpoint-config-prod-instance-count

Verifica se as configurações de SageMaker endpoint da Amazon têm variantes de produção `InitialInstanceCount` definidas com um valor maior que 1. A regra é NON_COMPLIANT se as variantes de produção `InitialInstanceCount` forem iguais a 1.

Identificador: SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUNT

Tipos de recursos: AWS::SageMaker::EndpointConfig

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

sagemaker-notebook-instance-inside-vpc

Verifica se uma instância de SageMaker notebook da Amazon foi iniciada em uma VPC ou em uma lista de sub-redes aprovadas. A regra será NON_COMPLIANT se uma instância de caderno não for iniciada em uma VPC ou se sua ID de sub-rede não estiver incluída na lista de parâmetros.

Identificador: SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

SubnetIds (Opcional), Tipo: Csv

> Lista separada por vírgulas de IDs de sub-rede em que as instância de caderno podem ser executadas.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sagemaker-notebook-instance-kms-key-configured

Verifica se uma AWS chave do Key Management Service (AWS KMS) está configurada para uma instância de SageMaker notebook da Amazon. A regra é NON_COMPLIANT se 'KmsKeyId' não for especificado para a instância do notebook. SageMaker

Identifier (Identificador): SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

Tipos de recursos: AWS::SageMaker::NotebookInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: string

> Lista separada por vírgula de ARNs de chave AWS KMS permitida para uma instância de notebook da Amazon. SageMaker

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sagemaker-notebook-instance-root-access-check

Verifica se a SageMaker RootAccess configuração da Amazon está habilitada para instâncias de SageMaker notebooks da Amazon. A regra é NON_COMPLIANT se a RootAccess configuração estiver definida como 'Ativada' para uma instância de notebook da Amazon SageMaker .

Identificador: SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

Tipos de recursos: AWS::SageMaker::NotebookInstance

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sagemaker-notebook-no-direct-internet-access

Verifica se o acesso direto à Internet está desativado para uma instância de SageMaker notebook da Amazon. A regra é NON_COMPLIANT se uma instância do SageMaker notebook estiver habilitada para Internet.

Identifier (Identificador): SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

Tipos de recursos: AWS::SageMaker::NotebookInstance

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

secretsmanager-rotation-enabled-check

Verifica se o segredo do AWS Secrets Manager tem a rotação ativada. A regra também verifica um parâmetro `maximumAllowedRotationFrequency` opcional. Se o parâmetro for especificado, a frequência de rotação do segredo será comparada com a frequência máxima permitida. A regra será NON_COMPLIANT se o segredo não estiver agendado para rotação. A regra também

é NON_COMPLIANT se a frequência de rotação for maior que o número especificado no maximumAllowedRotation parâmetro Frequência.

> **Note**
>
> Reavaliar essa regra em até 4 horas após a primeira avaliação não terá efeito sobre os resultados.

Identifier (Identificador): SECRETSMANAGER_ROTATION_ENABLED_CHECK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo AllowedRotationFrequency (opcional), Tipo: int

Frequência máxima permitida de rotação do segredo em dias.

máximo AllowedRotationFrequencyInHours (opcional), Tipo: int

Frequência máxima permitida de alternância do segredo em dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

secretsmanager-scheduled-rotation-success-check

Verifica se AWS os segredos do Secrets Manager foram rotacionados com sucesso de acordo com o cronograma de rotação. O Secrets Manager calcula a data em que a alternância deve acontecer. A regra será NON_COMPLIANT se a data passar e o segredo não for alternado.

> **Note**
>
> A regra retornar NOT_APPLICABLE para segredos sem alternância.

Identifier (Identificador): SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

secretsmanager-secret-periodic-rotation

Verifica se AWS os segredos do Secrets Manager foram alternados nos últimos dias especificados. A regra é NON_COMPLIANT se um segredo não tiver sido alternado por mais do que o número de dias de maxDaysSince rotação. O valor padrão é 90 dias.

Identificador: SECRETSMANAGER_SECRET_PERIODIC_ROTATION

Tipos de recursos: AWS::SecretsManager::Secret

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

máximo DaysSinceRotation (opcional), Tipo: int

> Número máximo de dias em que um segredo pode permanecer inalterado. O valor padrão é 90 dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

secretsmanager-secret-unused

Verifica se AWS os segredos do Secrets Manager foram acessados dentro de um determinado número de dias. A regra é NON_COMPLIANT se um segredo não tiver sido acessado em um número de dias 'não utilizado'ForDays. O valor padrão é 90 dias.

Contexto: é recomendável excluir rotineiramente segredos não utilizados. Segredos não utilizados podem ser usados indevidamente por antigos usuários que não precisam mais acessar esses segredos. Além disso, à medida que mais usuários obtêm acesso a um segredo, torna-se cada vez mais possível que alguém tenha usado indevidamente um segredo ou tenha concedido acesso a uma entidade não autorizada. A exclusão de segredos não utilizados ajuda a revogar o acesso secreto de usuários que não precisam mais dele e pode reduzir seu custo de uso. AWS Secrets Manager

Identificador: SECRETSMANAGER_SECRET_UNUSED

Tipos de recursos: AWS::SecretsManager::Secret

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

unusedForDays (Opcional), Tipo: int

O número de dias em que um segredo pode permanecer sem uso. O valor padrão é 90 dias.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

secretsmanager-using-cmk

Verifica se todos os segredos AWS Secrets Manager estão criptografados usando o Chave gerenciada pela AWS (`aws/secretsmanager`) ou uma chave gerenciada pelo cliente que foi criada em AWS Key Management Service (AWS KMS). A regra será COMPLIANT se um segredo for criptografado usando uma chave gerenciada pelo cliente. Essa regra será NON_COMPLIANT se um segredo for criptografado usando o `aws/secretsmanager`.

> **Note**
>
> Essa regra não tem acesso às chaves gerenciadas pelo cliente em várias contas e avalia os segredos como NON_COMPLIANT quando uma chave entre contas é usada.

Identificador: SECRETSMANAGER_USING_CMK

Tipos de recursos: AWS::SecretsManager::Secret

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyArns (Opcional), Tipo: Csv

Lista separada por vírgulas dos nomes dos recursos da Amazon (ARN) da chave do KMS para verificar se as chaves são usadas na criptografia.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

securityhub-enabled

Verifica se o AWS Security Hub está habilitado para uma AWS conta. A regra é NON_COMPLIANT se o AWS Security Hub não estiver habilitado.

Identificador: SECURITYHUB_ENABLED

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

security-account-information-provided

Verifica se você forneceu informações de contato de segurança para os contatos AWS da sua conta. A regra será NON_COMPLIANT se as informações de contato de segurança na conta não forem fornecidas.

Identificador: SECURITY_ACCOUNT_INFORMATION_PROVIDED

Tipos de recursos: AWS::::Account

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

catálogo de serviços compartilhado dentro da organização

Verifica se o AWS Service Catalog compartilha portfólios com uma organização (um conjunto de AWS contas tratadas como uma única unidade) quando a integração está habilitada com AWS Organizations. A regra é NON_COMPLIANT se o valor `Tipo` de uma ação for `ACCOUNT`.

Identificador: SERVICE_CATALOG_SHARED_WITHIN_ORGANIZATION

Tipos de recursos: AWS::ServiceCatalog::Portfolio

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

service-vpc-endpoint-enabled

Verifica se o endpoint de serviço para o serviço fornecido no parâmetro de regra é criado para cada Amazon Virtual Private Cloud (Amazon VPC). A regra retornará NON_COMPLIANT se uma Amazon VPC não tiver um endpoint da Amazon VPC criado para o serviço.

Identifier (Identificador): SERVICE_VPC_ENDPOINT_ENABLED

Tipos de recursos: AWS: :EC2: :VPC

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

serviceName, Tipo: string

> O nome abreviado ou o sufixo para o serviço. Nota: Para obter uma lista de nomes de serviços disponíveis ou uma lista de sufixos válida, use DescribeVpcEndpointServices.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ses-malware-scanning-enabled

Verifica se a verificação de malware e spam no recebimento de mensagens está habilitada no Amazon Simple Email Service (Amazon SES). A regra será NON_COMPLIANT se a verificação de malware e spam não estiver habilitada.

Identificador: SES_MALWARE_SCANNING_ENABLED

Tipos de recursos: AWS::SES::ReceiptRule

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na região da Europa (Irlanda), Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

shield-advanced-enabled-autorenew

Verifica se o AWS Shield Advanced está ativado em sua AWS conta e se essa assinatura está configurada para ser renovada automaticamente. A regra será COMPLIANT se o Shield Advanced estiver habilitado e a renovação automática estiver habilitada.

> **Note**
>
> O endpoint da API do só AWS Shield Advanced está disponível na região Leste dos EUA (Norte da Virgínia). Essa regra só deve ser programada para execução na região Leste dos EUA (Norte da Virgínia).

Identifier (Identificador): SHIELD_ADVANCED_ENABLED_AUTORENEW

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

shield-drt-access

Verifica se a Shield Response Team (SRT) pode acessar sua AWS conta. A regra é NON_COMPLIANT se AWS Shield Advanced estiver ativada, mas a função para acesso ao SRT não estiver configurada.

Identifier (Identificador): SHIELD_DRT_ACCESS

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sns-encrypted-kms

Verifica se os tópicos do SNS estão criptografados com o AWS Key Management Service (AWS KMS). A regra é NON_COMPLIANT se um tópico do SNS não estiver criptografado com o KMS. AWS Opcionalmente, especifique os ARNs da chave, os ARNs do alias, o nome do alias ou os IDs da chave para a regra verificar.

Identificador: SNS_ENCRYPTED_KMS

Tipos de recursos: AWS::SNS::Topic

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

kmsKeyIds (Opcional), Tipo: Csv

Lista separada por vírgula de nomes de recursos da Amazon (ARNs) da AWS chave KMS, ARNs de alias de KMS, nomes de alias de KMS ou IDs de chave KMS para a regra verificar.

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

sns-topic-message-delivery-notification-enabled

Verifica se o registro em log do Amazon Simple Notification Service (SNS) está habilitado para o status de entrega das mensagens de notificação enviadas para um tópico para os endpoints. A regra será NON_COMPLIANT se a notificação do status de entrega das mensagens não estiver habilitada.

Identificador: SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

Tipos de recursos: AWS::SNS::Topic

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

ssm-document-not-public

Verifica se AWS os documentos do Systems Manager pertencentes à conta são públicos. A regra será NON_COMPLIANT se os documentos do Systems Manager com o proprietário 'Próprio' forem públicos.

Identificador: SSM_DOCUMENT_NOT_PUBLIC

Tipos de recursos: AWS::SSM::Document

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

step-functions-state-machine-logging-enabled

Verifica se AWS a máquina Step Functions tem o registro ativado. A regra será NON_COMPLIANT se uma máquina de estado não tiver o registro em log habilitado ou se a configuração de registro em log não estiver no nível mínimo fornecido.

Identificador: STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

Tipos de recursos: AWS::StepFunctions::StateMachine

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

nuvem WatchLogGroupArns (opcional), Tipo: Csv

Lista separada por vírgula de nomes de recursos da Amazon (ARNs) para grupos de log do Amazon CloudWatch Logs. A regra verifica se os grupos de logs especificados estão configurados para os logs de estado da máquina.

logLevel (opcional), Tipo: string

O nível mínimo de log para sua máquina de estado. Os valores válidos incluem: ALL, ERROR, FATAL.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

storagegateway-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para volumes do AWS Storage Gateway. A regra será NON_COMPLIANT se o volume do Storage Gateway não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::StorageGateway::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags dos volumes do Storage Gateway para verificação da regra, no formato JSON `{"tagkey" : "tagValue"}`.

resourceId (opcional), Tipo: string

ID do volume do Storage Gateway para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

storagegateway-resources-protected-by-backup-plan

Verifica se os volumes do AWS Storage Gateway estão protegidos por um plano de backup. A regra será NON_COMPLIANT se o volume do Storage Gateway não estiver coberto por um plano de backup.

Identificador: STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::StorageGateway::Volume

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para volumes do Storage Gateway para verificação da regra, no formato JSON.

resourceId (opcional), Tipo: string

ID do volume do Storage Gateway para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

subnet-auto-assign-public-ip-disabled

Verifica se as sub-redes do Amazon Virtual Private Cloud (Amazon VPC) recebem um endereço IP público. A regra será COMPLIANT se a Amazon VPC não tiver sub-redes que recebem um endereço IP público. A regra será NON_COMPLIANT se a Amazon VPC tiver sub-redes que recebem um endereço IP público.

Identificador: SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

Tipos de recursos: AWS::EC2::Subnet

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

Avaliação proativa

Para ver as etapas sobre como executar essa regra no modo proativo, consulte Avaliando seus recursos com AWS Config regras. Para que essa regra retorne COMPLIANT no modo proativo, o esquema de configuração de recursos da API de StartResourceavaliação precisa incluir as seguintes entradas, codificadas como uma string:

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

Para obter mais informações sobre avaliação proativa, consulte Modo de avaliação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

transfer-family-server-no-ftp

Verifica se um servidor criado com o AWS Transfer Family usa FTP para conexão de endpoint. A regra é NON_COMPLIANT se o protocolo do servidor para conexão de endpoint estiver habilitado para FTP.

Identificador: TRANSFER_FAMILY_SERVER_NO_FTP

Tipos de recursos: AWS::Transfer::Server

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

virtualmachine-last-backup-recovery-point-created

Verifica se um ponto de recuperação foi criado para o AWS VirtualMachines Backup-Gateway. A regra é NON_COMPLIANT se um AWS gateway de backup VirtualMachines não tiver um ponto de recuperação correspondente criado dentro do período especificado.

Identificador: VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

Tipos de recursos: AWS::BackupGateway::VirtualMachine

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags do AWS Backup-Gateway VirtualMachines para a regra verificar, no formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opcional), Tipo: string

ID do AWS Backup-Gateway VirtualMachine para verificação da regra.

recuperação PointAgeValue (opcional), Tipo: int, Padrão: 1

Valor numérico para a idade máxima permitida. Não mais do que 744 para horas, 31 para dias.

recuperação PointAgeUnit (opcional), Tipo: string, Padrão: dias

Unidade de tempo para a idade máxima permitida. Valores aceitos: 'horas', 'dias'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

virtualmachine-resources-protected-by-backup-plan

Verifica se o AWS Backup-Gateway VirtualMachines está protegido por um plano de backup. A regra é NON_COMPLIANT se o Backup-Gateway não VirtualMachine estiver coberto por um plano de backup.

Identificador: VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

Tipos de recursos: AWS::BackupGateway::VirtualMachine

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

resourceTags (opcional), Tipo: string

Tags para AWS Backup-Gateway VirtualMachines para a regra verificar, no formato JSON. `{"tagkey" : "tagValue"}`

resourceId (opcional), Tipo: string

ID do AWS Backup-Gateway VirtualMachine para verificação da regra.

crossRegionList (Opcional), Tipo: string

Lista separada por vírgulas das regiões de destino para a cópia de backup entre regiões a ser mantida

crossAccountList (Opcional), Tipo: string

Lista separada por vírgulas de contas de destino para manter uma cópia de backup entre contas

maxRetentionDays (Opcional), Tipo: int

O período máximo de retenção em dias para a Trava de Segurança do Backup

minRetentionDays (Opcional), Tipo: int

O período mínimo de retenção em dias para a Trava de Segurança do Backup

backup VaultLockCheck (opcional), Tipo: string

Valores aceitos: 'True' ou 'False'. Digite 'True' para que a regra verifique se o backup do recurso está em um cofre trancado

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

vpc-default-security-group-closed

Verifica se o grupo de segurança padrão de qualquer Amazon Virtual Private Cloud (Amazon VPC) não permite tráfego de entrada ou de saída. A regra será NON_COMPLIANT se o grupo de segurança padrão tiver um ou mais tráfegos de entrada ou de saída.

> **Note**
>
> Pode haver um atraso entre os AWS Config registros da exclusão de recursos relacionados, como grupos de segurança padrão, que são excluídos como parte da exclusão da Amazon VPC. Como resultado, mesmo que todos os grupos de segurança padrão ou outros recursos relacionados tenham sido excluídos ou corrigidos, a regra poderá relatar NON_COMPLIANT até o próximo processo de definição de base da conta.

Identifier (Identificador): VPC_DEFAULT_SECURITY_GROUP_CLOSED

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

vpc-flow-logs-enabled

Verifica se os logs de fluxo do Amazon Virtual Private Cloud (Amazon VPC) foram encontrados e habilitados para todas as Amazon VPCs. A regra é NON_COMPLIANT se os logs de fluxo não estiverem habilitados para pelo menos uma Amazon VPC.

Identifier (Identificador): VPC_FLOW_LOGS_ENABLED

Tipos de recursos: AWS: :EC2: :VPC

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

trafficType (opcional), Tipo: string

TrafficType de registros de fluxo

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

vpc-network-acl-unused-check

Verifica se há listas de controle de acesso à rede (ACLs de rede) não utilizadas. A regra será COMPLIANT se cada Network ACL estiver associada a uma sub-rede. A regra é NON_COMPLIANT se uma ACL de rede não estiver associada a uma sub-rede.

Identificador: VPC_NETWORK_ACL_UNUSED_CHECK

Tipos de recursos: AWS::EC2::NetworkAcl

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

vpc-peering-dns-resolution-check

Verifica se a resolução de DNS da VPC aceitante/solicitante para o IP privado está habilitada. A regra será NON_COMPLIANT se a resolução de DNS da VPC aceitante/solicitante para o IP privado não estiver habilitada.

Identificador: VPC_PEERING_DNS_RESOLUTION_CHECK

Tipos de recursos: AWS: :EC2: :VPC PeeringConnection

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

vpcIds (opcional), Tipo: Csv

Lista separada por vírgulas de IDs de VPC para verificação.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

vpc-sg-open-only-to-authorized-ports

Verifica se os grupos de segurança que permitem tráfego de entrada irrestrito ('0.0.0.0/0' ou '::/0') só permitem conexões TCP ou UDP de entrada em portas autorizadas. A regra será NON_COMPLIANT se esses grupos de segurança não tiverem portas especificadas nos parâmetros da regra.

> **Note**
>
> Essa regra avalia grupos de segurança do Amazon EC2 com regra de entrada definida como IPv4='0.0.0.0/0' or IPv6='::/'. Se o grupo de segurança não tiver um desses destinos, essa regra retornará `NOT_APPLICABLE`.

Identifier (Identificador): VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

Tipos de recursos: AWS::EC2::SecurityGroup

Tipo de trigger: alterações da configuração e da periodicidade

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

authorizedTcpPorts (Opcional), Tipo: string

Lista separada por vírgulas das portas TCP autorizadas a serem abertas para 0.0.0.0/0 ou ::/0. Os intervalos são definidos por traços, por exemplo, "443,1020-1025".

authorizedUdpPorts (Opcional), Tipo: string

Lista separada por vírgulas das portas UDP autorizadas a serem abertas para 0.0.0.0/0 ou ::/0. Os intervalos são definidos por traços, por exemplo, "500,1020-1025".

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

verificação de restrição de porta vpc-sg-

Verifica se os grupos de segurança restringem explicitamente o tráfego de entrada para portas restritas de 0.0.0.0/0 ou: :/0. A regra é NON_COMPLIANT se os grupos de segurança permitirem tráfego de entrada de 0.0.0.0/0 ou: :/0 pelas portas TCP/UDP 22/3389 ou conforme especificado nos parâmetros.

Identificador: VPC_SG_PORT_RESTRICTION_CHECK

Tipos de recursos: AWS::EC2::SecurityGroup

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Restringir portas (opcional), Tipo: Csv

Lista separada por vírgulas de portas que não devem estar abertas para tráfego de entrada em toda a faixa de IP. Os números de porta válidos variam de 0 a 65535. Se não for especificada, o padrão da regra é verificar 22 e 3389.

Tipo de protocolo (opcional), Tipo: string

O tipo de protocolo de transmissão a ser verificado pela regra. Os valores válidos incluem 'TCP', 'UDP' e 'ALL' (sem distinção entre maiúsculas e minúsculas). Se definida como 'ALL', a regra verificará as regras que usam o protocolo 'TCP', 'UDP' ou 'ALL' (-1). O valor padrão é 'ALL'.

excluir ExternalSecurityGroups (opcional), Tipo: booliano

Sinalizador booleano para excluir a avaliação de grupos de segurança externos. Se definida como 'true', a regra não incluirá grupos de segurança externos na avaliação. Caso contrário,

todos os grupos de segurança serão avaliados se o valor for definido como 'falso'. O valor padrão é 'verdadeiro'.

Tipo de IP (opcional), Tipo: string

A versão do Protocolo de Internet (IP) para verificação da regra. Os valores válidos incluem 'IPv4', 'IPv6' e 'ALL' (sem distinção entre maiúsculas e minúsculas). Se não for especificada, o padrão da regra é verificar 'ALL'.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

vpc-vpn-2-tunnels-up

Verifica se os dois túneis de rede privada virtual (VPN) fornecidos pela VPN AWS Site-to-Site estão no status UP. A regra retornará NON_COMPLIANT se um ou ambos os túneis estiverem no status DOWN.

Identifier (Identificador): VPC_VPN_2_TUNNELS_UP

Tipos de recursos: AWS::EC2::VPNConnection

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

wafv2-logging-enabled

Verifica se o registro está habilitado nas listas de controle de acesso à web regionais e globais (ACLs da web) do AWS WAFv2. A regra será NON_COMPLIANT se o registro em log estiver habilitado, mas o destino do registro não corresponder ao valor do parâmetro.

Identificador: WAFV2_LOGGING_ENABLED

Tipos de recursos: AWS::WAFv2::Web ACL

Trigger type (Tipo de trigger): periódico

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

KinesisFirehoseDeliveryStreamArns (Opcional), Tipo: Csv

Lista separada por vírgulas dos ARNs do fluxo de entrega do Kinesis Firehose

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

wafv2-rulegroup-logging-enabled

Verifica se a coleta CloudWatch de métricas de segurança da Amazon em grupos de regras do AWS WAFv2 está ativada. A regra é NON_COMPLIANT se o '. VisibilityConfig CloudWatchMetricsEnabledO campo 'está definido como falso.

Contexto: AWS WAFV2 (Web Application Firewall versão 2) permite criar AWS WAF regras para proteger seus aplicativos da Web contra explorações e vulnerabilidades comuns da Web. Um grupo de AWS WAF regras é uma coleção de AWS WAF regras que você pode associar a uma Web ACL (Access Control List) para definir o comportamento desejado para o tráfego do seu aplicativo web. Para obter mais informações, consulte AWS WAF regras e grupos de regras no Guia do AWS WAF desenvolvedor.

Ao configurar a coleta de métricas de CloudWatch segurança no grupo de AWS WAFV2 regras, você pode monitorar métricas de segurança, como ataques bem-sucedidos ou malsucedidos de negação de serviço distribuído (DDoS), injeção de SQL e scripts entre sites (XSS). As métricas de segurança coletadas podem ajudar você a simplificar suas investigações.

> **Note**
>
> Se não houver AWS WAF regras no grupo de regras para a AWS WAFV2 regra gerenciada verificar, a regra AWS Config gerenciada retornará AWS Config NON_APPLICABLE.

Identificador: WAFV2_RULEGROUP_LOGGING_ENABLED

Tipos de recursos: AWS::WAFv2::RuleGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

wafv2-rulegroup-not-empty

Verifica se os grupos de regras do WAFv2 contêm regras. A regra será NON_COMPLIANT se não houver regras em um grupo de regras do WAFv2.

Identificador: WAFV2_RULEGROUP_NOT_EMPTY

Tipos de recursos: AWS::WAFv2::RuleGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

wafv2-webacl-not-empty

Verifica se uma ACL da web do WAFv2 contém alguma regra do WAF ou grupos de regras do WAF. Essa regra será NON_COMPLIANT se uma ACL da web não contiver nenhuma regra WAF ou grupos de regras do WAF.

Identificador: WAFV2_WEBACL_NOT_EMPTY

Tipos de recursos: AWS::WAFv2::Web ACL

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulte[Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation](#).

waf-classic-logging-enabled

Verifica se o registro está habilitado nas listas de controle de acesso à web globais clássicas do AWS WAF (ACLs da web). A regra será NON_COMPLIANT para uma ACL global da web se ela não tiver o registro em log habilitado.

Identificador: WAF_CLASSIC_LOGGING_ENABLED

Tipos de recursos: AWS::WAF::Web ACL

Trigger type (Tipo de trigger): periódico

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

KinesisFirehoseDeliveryStreamArns (Opcional), Tipo: Csv

Lista separada por vírgulas do ARN do stream do Amazon Kinesis para registros do AWS WAF.

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-global-rulegroup-not-empty

Verifica se um grupo de regras AWS do WAF Classic contém alguma regra. A regra será NON_COMPLIANT se não houver regras presentes em um grupo de regras.

Identificador: WAF_GLOBAL_RULEGROUP_NOT_EMPTY

Tipos de recursos: AWS::WAF::RuleGroup

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-global-rule-not-empty

Verifica se uma regra global AWS do WAF contém alguma condição. A regra será NON_COMPLIANT se nenhuma condição estiver presente na regra global do WAF.

Identificador: WAF_GLOBAL_RULE_NOT_EMPTY

Tipos de recursos: AWS::WAF::Rule

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-global-webacl-not-empty

Verifica se uma ACL da web do WAF Global contém regras ou grupo de regras do WAF. Essa regra será NON_COMPLIANT se uma ACL da web não contiver nenhuma regra ou grupo de regras do WAF.

Identificador: WAF_GLOBAL_WEBACL_NOT_EMPTY

Tipos de recursos: AWS::WAF::Web ACL

Tipo de trigger: alterações da configuração

Região da AWS: somente disponível na região Leste dos EUA (Norte da Virgínia)

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-regional-rulegroup-not-empty

Verifica se os grupos de regras regionais do WAF contêm alguma regra. A regra será NON_COMPLIANT se não houver regras presentes em um grupo de regras regionais do WAF.

Identificador: WAF_REGIONAL_RULEGROUP_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::RuleGroup

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-regional-rule-not-empty

Verifica se a regra regional do WAF contém condições. Essa regra será COMPLIANT se a regra regional contiver pelo menos uma condição e, caso contrário, será NON_COMPLIANT.

Identificador: WAF_REGIONAL_RULE_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::Rule

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

waf-regional-webacl-not-empty

Verifica se uma ACL da web regional do WAF contém alguma regra ou grupos de regras do WAF. A regra será NON_COMPLIANT se não houver regras ou grupos de regras do WAF presentes em uma ACL da web.

Identificador: WAF_REGIONAL_WEBACL_NOT_EMPTY

Tipos de recursos: AWS::WAFRegional::Web ACL

Tipo de trigger: alterações da configuração

Região da AWS: Todas as AWS regiões suportadas

Parâmetros:

Nenhum

AWS CloudFormation modelo

Para criar regras AWS Config gerenciadas com AWS CloudFormation modelos, consulteCriar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.

Lista de regras AWS Config gerenciadas por modo de avaliação

AWS Config atualmente oferece suporte às seguintes regras gerenciadas.

Considerações

Valores padrão para regras gerenciadas

Os valores padrão especificados para regras gerenciadas são pré-preenchidos somente ao usar o AWS console. Os valores padrão não são fornecidos para a API, a CLI ou o SDK.

Não há suporte para buckets de diretório

As regras gerenciadas só oferecem suporte a buckets de uso geral ao avaliar os recursos do Amazon Simple Storage Service (Amazon S3). AWS Config não registra alterações de configuração para buckets de diretório. Para obter mais informações sobre buckets de uso geral e buckets de diretório, consulte Visão geral dos buckets e Buckets de diretório no Guia do usuário do Amazon S3.

Regras gerenciadas e tipos de recursos globais do IAM

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Avaliação proativa

Regras proativas são regras que oferecem suporte ao modo de avaliação proativa para recursos que não foram implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região. Para obter mais informações, consulte Modos de avaliação.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Avaliação proativa

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check

- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled

Avaliação de detecção

Regras de detecção são regras que são compatíveis com o modo de avaliação de detecção para o recurso que já foi implantado. Isso permite avaliar as definições de configuração de seus recursos existentes.

> **Note**
>
> Atualmente, todas as AWS Config regras apoiam a avaliação de detetives.

Avaliação de detecção

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted

- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check

- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch

- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings

- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- verificação de expiração do certificado do servidor iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check

- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Lista de regras AWS Config gerenciadas por tipo de acionador

AWS Config atualmente oferece suporte às seguintes regras gerenciadas.

Considerações

Valores padrão para regras gerenciadas

Os valores padrão especificados para regras gerenciadas são pré-preenchidos somente ao usar o AWS console. Os valores padrão não são fornecidos para a API, a CLI ou o SDK.

Não há suporte para buckets de diretório

As regras gerenciadas só oferecem suporte a buckets de uso geral ao avaliar os recursos do Amazon Simple Storage Service (Amazon S3). AWS Config não registra alterações de configuração para buckets de diretório. Para obter mais informações sobre buckets de uso geral e buckets de diretório, consulte Visão geral dos buckets e Buckets de diretório no Guia do usuário do Amazon S3.

Regras gerenciadas e tipos de recursos globais do IAM

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as

regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas. Para obter uma lista de quais regras gerenciadas são suportadas em quais regiões, consulte Lista de regras AWS Config gerenciadas por disponibilidade regional.

Alterações de configuração

As regras acionadas por alterações são regras que são AWS Config avaliadas em resposta às alterações de configuração.

Alterações de configuração

- acm-certificate-rsa-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-client-vpn-connection-log-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- global-endpoint-event-replication-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- catálogo de serviços compartilhado dentro da organização
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty

- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Periódico

As regras periódicas são regras que são AWS Config avaliadas periodicamente com uma frequência especificada por você; por exemplo, a cada 24 horas.

Periódico

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- verificação de expiração do certificado do servidor iam
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- kinesis-firehose-delivery-stream criptografado
- kms-cmk-not-scheduled-for-deletion
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- rds-in-backup-plan

- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-resources-protected-by-backup-plan
- redshift - acesso irrestrito à porta
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-flow-logs-enabled
- verificação de restrição de porta vpc-sg-

- wafv2-logging-enabled
- waf-classic-logging-enabled

Híbrida

As regras híbridas são regras que AWS Config avaliam tanto em resposta às mudanças de configuração quanto periodicamente.

Híbrida

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

Disponibilidade da lista de regras AWS Config gerenciadas por região

AWS Config atualmente oferece suporte às seguintes regras gerenciadas.

Considerações

Valores padrão para regras gerenciadas

Os valores padrão especificados para regras gerenciadas são pré-preenchidos somente ao usar o AWS console. Os valores padrão não são fornecidos para a API, a CLI ou o SDK.

Não há suporte para buckets de diretório

As regras gerenciadas só oferecem suporte a buckets de uso geral ao avaliar os recursos do Amazon Simple Storage Service (Amazon S3). AWS Config não registra alterações de configuração para buckets de diretório. Para obter mais informações sobre buckets de uso geral e buckets de diretório, consulte Visão geral dos buckets e Buckets de diretório no Guia do usuário do Amazon S3.

Regras gerenciadas e tipos de recursos globais do IAM

Os tipos de recursos globais do IAM integrados antes de fevereiro de 2022 (`AWS::IAM::Group`,, `AWS::IAM::PolicyAWS::IAM::Role`, e`AWS::IAM::User`) só podem ser registrados AWS nas regiões AWS Config em que AWS Config estavam disponíveis antes de fevereiro de 2022. Esses tipos de recursos não podem ser registrados nas regiões com suporte AWS Config após fevereiro de 2022. Para obter uma lista dessas regiões, consulte AWS Recursos de gravação | Recursos globais.

Se você registrar um tipo de recurso global do IAM em pelo menos uma região, as regras periódicas que relatam a conformidade com o tipo de recurso global do IAM executarão avaliações em todas as regiões em que a regra periódica for adicionada, mesmo que você não tenha ativado o registro do tipo de recurso global do IAM na região em que a regra periódica foi adicionada.

Para evitar avaliações desnecessárias, você só deve implantar regras periódicas que relatem a conformidade em um tipo de recurso global do IAM para uma das regiões suportadas.

Região Leste dos EUA (Ohio)

Leste dos EUA (Ohio)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check

- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured

- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check

- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Leste dos EUA (N. da Virgínia)

Leste dos EUA (Norte da Virgínia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled

- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled

- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions

- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- verificação de expiração do certificado do servidor iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created

- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty

- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Oeste dos EUA (Norte da Califórnia)

Oeste dos EUA (N. da Califórnia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized

- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Oeste dos EUA (Oregon)

Oeste dos EUA (Oregon)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled

- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging

- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit

- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized

- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted

- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited

- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região África (Cidade do Cabo)

África (Cidade do Cabo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption

- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- habilitado para dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access

- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Hong Kong)

Ásia-Pacífico (Hong Kong)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled

- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check

- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled

- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Ásia-Pacífico (Haiderabade)

Ásia-Pacífico (Hyderabad)

- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag

- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled

- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream criptografado
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Região Ásia-Pacífico (Jacarta)

Ásia-Pacífico (Jacarta)

- access-keys-rotated
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-multiple-az
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check

- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- kinesis-firehose-delivery-stream criptografado
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-default-admin-check
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- step-functions-state-machine-logging-enabled

- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

Região Ásia-Pacífico (Melbourne)

Ásia-Pacífico (Melbourne)

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw

- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3

- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Mumbai)

Ásia-Pacífico (Mumbai)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured

- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Osaka)

Ásia-Pacífico (Osaka)

- access-keys-rotated
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types

- clb-desync-mode-check
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db

- habilitado para dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-launch-template-public-ip-disabled
- ec2-no-amazon-key-pair
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecs-containers-readonly-access
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit

- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elbv2-multiple-az
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-cluster-default-admin-check
- rds-cluster-encrypted-at-rest
- rds-instance-default-admin-check
- rds-instance-public-access-check
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- habilitado para replicação entre regiões de buckets s3
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-peering-dns-resolution-check
- verificação de restrição de porta vpc-sg-
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Seul)

Ásia-Pacífico (Seul)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured

- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication

- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check

- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty

- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Singapura)

Ásia-Pacífico (Singapura)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db

- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Sydney)

Ásia-Pacífico (Sydney)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type

- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled

- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado

- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check

- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports

- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Ásia-Pacífico (Tóquio)

Ásia-Pacífico (Tóquio)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check

- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled

- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Canadá (Central)

Canadá (Central)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket-cloudtrail-s3-bucket-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target

- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled

- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check

- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check

- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check

- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl

- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check

- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Oeste do Canadá (Calgary)

Oeste do Canadá (Calgary)

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- approved-amis-by-id
- approved-amis-by-tag
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- eip-attached
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled

- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

Região China (Pequim)

China (Pequim)

- access-keys-rotated

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- registro de acesso ao bucket-cloudtrail-s3-bucket-

- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região China (Ningxia)

China (Ningxia)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check

- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled

- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc

- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

Região Europa (Frankfurt)

Europa (Frankfurt)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created

- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado

- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks

- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Irlanda)

Europa (Irlanda)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3-
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db

- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled

- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured

- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted

- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled

- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Londres)

Europa (Londres)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag

- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado

- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags

- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured

- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Milão)

Europa (Milão)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest

- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- habilitado para dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted

- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift - acesso irrestrito à porta

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Paris)

Europa (Paris)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled

- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized

- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled

- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Espanha)

Europa (Espanha)

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-log-enabled

- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream criptografado
- multi-region-cloud-trail-enabled

- nacl-no-unrestricted-ssh-rdp
- rds-instance-default-admin-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ssm-document-not-public

- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Região Europa (Estocolmo)

Europa (Estocolmo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id

- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls

- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity

- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required

- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada

- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento de código lambda do inspetor
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check

- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets

- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região Europa (Zurique)

Europa (Zurique)

- account-part-of-organizations

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-mount-target-public-accessible
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- elb-deletion-protection-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado

- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-external-access analyzer habilitado
- iam-password-policy
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-snapshot-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Região de Israel (Tel Aviv)

Israel (Tel Aviv)

- account-part-of-organizations

- alb-desync-mode-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- eip-attached
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- proteção guardduty-s3 ativada
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- verificação automática de descoberta de dados com sensibilidade automática
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- verificação de restrição de porta vpc-sg-
- wafv2-webacl-not-empty

Região Oriente Médio (Bahrein)

Oriente Médio (Barém)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada

- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited

- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public

- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Região do Oriente Médio (Emirados Árabes Unidos)

Oriente Médio (Emirados Árabes Unidos)

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs-mount-target-public-accessible
- eks-cluster-log-enabled

- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada

- iam-external-access analyzer habilitado
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-rabbit-deployment-mode
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled

- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-instance-count
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

Região América do Sul (São Paulo)

América do Sul (São Paulo)

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- criptografia de endpoint dax-tls-
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- guardduty-eks-protection-audit-habilitado
- guardduty-eks-protection-runtime-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- proteção contra malware guardduty-habilitada
- guardduty-non-archived-findings
- proteção guardduty-rds-habilitada
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-external-access analyzer habilitado

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- verificação automática de descoberta de dados com sensibilidade automática

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-cloudwatch-audit-log-habilitado
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled

- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

AWS GovCloud Região (Leste dos EUA)

AWS GovCloud (Leste dos EUA)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada
- habilitado para dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check

- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created

- fsx-resources-protected-by-backup-plan
- guardduty-eks-protection-audit-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-habilitado
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catálogo de serviços compartilhado dentro da organização
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-

- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud Região (Oeste dos EUA)

AWS GovCloud (Oeste dos EUA)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check

- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- verificação de eventos de dados cloudtrail-all-read-s3
- cloudtrail-all-write-s3-data-event-check
- registro de acesso ao bucket do cloudtrail-s3-
- cloudtrail-s3-bucket-public-access proibido
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- habilitado para autenticação dms-mongo-db
- dms-neptune-iam com autorização habilitada

- habilitado para dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-mount-target-public-accessible
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- guardduty-eks-protection-audit-habilitado
- guardduty-enabled-centralized
- habilitado para proteção guardduty-lambda
- guardduty-non-archived-findings
- proteção guardduty-s3 ativada
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- verificação de expiração do certificado do servidor iam
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspetor-ec2-scan habilitado
- habilitado para inspector-ecr-scan
- habilitado para escaneamento padrão inspetor-lambda
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream criptografado
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-cloudwatch-audit-log-habilitado
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-tolerance
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift - acesso irrestrito à porta
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- habilitado para replicação entre regiões de buckets s3
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker-endpoint-config-prod-instance-count
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- catálogo de serviços compartilhado dentro da organização

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- verificação de restrição de porta vpc-sg-
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Regras vinculadas ao serviço AWS Config

Uma AWS Config regra vinculada a serviços é um tipo exclusivo de regras AWS Config gerenciadas que permite que outros AWS serviços criem AWS Config regras em sua conta. As regras vinculadas ao serviço são predefinidas para incluir todas as permissões necessárias para chamar outros AWS serviços em seu nome. Essas regras são semelhantes aos padrões que um AWS serviço recomenda em você Conta da AWS para verificação de conformidade.

Essas AWS Config regras vinculadas ao serviço são de propriedade das equipes de AWS serviço. A equipe AWS de serviço cria essas regras em seu Conta da AWS. Você tem acesso somente leitura a essas regras. Você não pode editar ou excluir essas regras se estiver inscrito em um AWS serviço ao qual essas regras estão vinculadas.

Regras vinculadas a serviços e o AWS Command Line Interface

Com o AWS CLI, as APIs PutConfigDeleteConfigRule, Rule e DeleteEvaluationResults retornam o acesso negado com a seguinte mensagem de erro:

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

Regras vinculadas a serviços e o console AWS Config

No AWS Config console, as AWS Config regras vinculadas ao serviço estão visíveis na página Regras. Os botões Editar e Excluir resultados estão acinzentados no console para impedir que você edite a regra. Você pode visualizar os detalhes da regra selecionando-a.

Regras vinculadas a serviços, ações de remediação e pacotes de conformidade

Para adicionar ações de remediação a regras vinculadas ao serviço em um pacote de conformidade, você precisa adicionar a ação de remediação ao próprio modelo do pacote de conformidade e, em seguida, atualizar o pacote de conformidade com seu modelo atualizado. Para obter informações sobre a atualização de pacotes de conformidade, consulte Implantando um pacote de conformidade (console), Implantando um pacote de conformidade ()e Gerenciando pacotes de conformidade organizacional.AWS CLI

Editando e excluindo regras vinculadas a serviços

Para editar ou excluir uma regra vinculada ao serviço, entre em contato com o AWS serviço que criou a regra. Por exemplo, para regras vinculadas a serviços criadas por AWS Security Hub, você pode remover uma regra vinculada a serviços seguindo estas etapas no Guia do AWS Security Hub usuário: Desabilitando um padrão de segurança.

Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation

> **Important**
>
> Você deve primeiro criar e iniciar o gravador deAWS Config configuração para criar regrasAWS Config gerenciadas comAWS CloudFormation. Para obter mais informações, consulte Gerenciar o gravador de configuração.

Para regras gerenciadas compatíveis do AWS Config, você pode usar os modelos do AWS CloudFormation para criar a regra para a sua conta ou atualizar uma pilha do AWS CloudFormation

existente. Uma pilha do é um conjunto de recursos relacionados que você provisiona e atualiza como uma unidade. Quando você executa uma pilha com um modelo, a regra gerenciada AWS Config é criada para você. Os modelos criam apenas a regra; eles não criam recursos adicionais AWS.

> **Note**
>
> Quando as regras gerenciadas AWS Config são atualizadas, os modelos são atualizados com as alterações mais recentes. Para salvar uma versão específica de um modelo para uma regra, faça download do modelo e faça upload dele para o seu bucket do S3.

Para obter mais informações sobre como trabalhar comAWS CloudFormation modelos, consulte IntroduçãoAWS CloudFormation no Guia doAWS CloudFormation usuário.

Para executar uma pilha do AWS CloudFormation para uma regra gerenciada do AWS Config

1. Vá até o CloudFormationconsole e crie uma nova pilha.
2. Para Specify template (Especificar modelo):
   - Se tiver feito download do modelo, selecione Upload a template file (Fazer upload de um arquivo de modelo) e Choose file (Escolher arquivo) para fazer upload do modelo.
   - Você também pode escolher o URL do Amazon S3 e inserir o URL do modelo`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/`*`THE_RULE_IDENTIFIER`*`.template`.

   > **Note**
   >
   > O identificador da regra deve ser escrito em ALL_CAPS_WITH_UNDERSCORES. Por exemplo, CLOUDWATCH_LOG_GROUP_ENCRYPTED em vez decloudwatch-log-group-encrypted.
   > Para algumas regras, o identificador da regra é diferente do nome da regra.
   > Use o identificação. Por exemplo, o identificador de regra para o ssh restrito é INCOMING_SSH_DISABLED.

3. Escolha Next (Próximo).
4. Em Specify stack details (Especificar detalhes da pilha), digite um nome de pilha e os valores de parâmetro para a regra do AWS Config. Por exemplo, se estiver usando o modelo de regra

gerenciada `DESIRED_INSTANCE_TYPE`, você pode especificar o tipo de instância; por exemplo, "m4.large".

5. Escolha Next (Próximo).
6. Em Options (Opções), você pode criar tags ou configurar outras opções avançadas. Elas não são obrigatórias.
7. Escolha Next (Próximo).
8. Em Review (Revisar), verifique se o modelo, os parâmetros e as outras opções estão corretas.
9. Escolha Create (Criar). A pilha é criada em alguns minutos. Você pode visualizar a regra criada no console do AWS Config.

Você pode usar os modelos para criar uma única pilha para as regras gerenciadas AWS Config ou atualizar uma pilha existente em sua conta. Se você excluir uma pilha, as regras gerenciadas criadas a partir dessa pilha também serão excluídas. Para obter mais informações, consulte Como trabalhar com pilhas no GuiaAWS CloudFormation do usuário.

AWS Config Regras personalizadas

AWS Config Regras personalizadas são regras que você cria do zero. Há duas maneiras de criar regras AWS Config personalizadas: com as funções Lambda (Guia do AWS Lambda desenvolvedor) e com o Guard (Guard GitHub Repository), uma linguagem. policy-as-code

AWS Config as regras personalizadas criadas com o Lambda são chamadas de Regras AWS Config Lambda AWS Config Personalizadas e as regras personalizadas criadas com o Guard são chamadas AWS Config de Regras de Política Personalizadas.

AWS Config Regras de política personalizadas

As regras escritas usando o Guard podem ser criadas no AWS Config console ou usando as APIs de AWS Config regras. AWS Config As regras de políticas personalizadas permitem que você crie regras AWS Config personalizadas sem precisar usar Java ou Python para desenvolver funções do Lambda e gerenciar suas regras personalizadas. AWS Config As regras de política personalizada são iniciadas por alterações de configuração. Para obter mais informações sobre o Guard, consulte o GitHubRepositório do Guard.

AWS Config Regras personalizadas do Lambda

As regras personalizadas do Lambda oferecem a opção de usar Java ou Python para criar uma função do Lambda para uma regra personalizada. AWS Config Uma função Lambda é um código personalizado para o qual você faz o AWS Lambda upload e é invocado por eventos que são publicados nela por uma fonte de eventos. Se a função Lambda estiver associada a uma AWS Config regra, ela será AWS Config invocada quando a regra for iniciada. Em seguida, a função Lambda avalia as informações de configuração enviadas por AWS Config e retorna os resultados da avaliação. Para mais informações sobre as funções do Lambda, consulte Origens de eventos e funções no Guia do desenvolvedor do AWS Lambda .

Considerações sobre custos

Para obter detalhes sobre os custos associados ao registro de recursos, consulte AWS Config preços.

Recomendação: adicione lógica para lidar com a avaliação de recursos excluídos para regras lambda personalizadas

Ao criar regras lambda AWS Config personalizadas, é altamente recomendável que você adicione lógica para lidar com a avaliação dos recursos excluídos.

Quando os resultados da avaliação forem marcados como `NOT_APPLICABLE`, eles serão marcados para exclusão e limpos. Se NÃO estiverem marcados como `NOT_APPLICABLE`, os resultados da avaliação permanecerão inalterados até que a regra seja excluída, o que pode causar um aumento inesperado na criação de itens de configuração (CIs) para o `AWS::Config::ResourceCompliance` após a exclusão da regra.

Para obter informações sobre como definir regras lambda AWS Config personalizadas para retornar `NOT_APPLICABLE` para recursos excluídos, consulte Gerenciamento de recursos excluídos com regras lambda AWS Config personalizadas.

Recomendação: forneça os recursos no escopo das regras lambda personalizadas

AWS Config As regras personalizadas do Lambda podem causar um grande número de invocações de funções do Lambda se a regra não tiver como escopo um ou mais tipos de recursos. Para evitar o aumento da atividade associada à sua conta, é altamente recomendável fornecer recursos no escopo de suas regras personalizadas do Lambda. Se nenhum tipo de recurso for selecionado, a regra invocará a função do Lambda para todos os recursos na conta.

Recomendação: pare de registrar a conformidade dos recursos antes de excluir as regras

É altamente recomendável que você interrompa a gravação do tipo de `AWS::Config::ResourceCompliance` recurso antes de excluir as regras da sua conta. A exclusão de regras cria CIs `AWS::Config::ResourceCompliance` e pode afetar os custos do gravador AWS Config de configuração. Se você estiver excluindo regras que avaliam um grande número de tipos de recursos, isso pode levar a um aumento no número de ICs registrados.

Prática recomendada:

1. Pare de gravar `AWS::Config::ResourceCompliance`
2. Excluir regra (s)
3. Ativar a gravação para `AWS::Config::ResourceCompliance`

Tipos de trigger

Depois de adicionar uma regra à sua conta, AWS Config compara seus recursos com as condições da regra. Após essa avaliação inicial, AWS Config continua executando avaliações cada vez que uma é acionada. Os gatilhos de avaliação são definidos como parte da regra e podem incluir os seguintes tipos.

Tipo de gatilho	Descrição
Alterações de configuração	AWS Config executa avaliações para a regra quando há um recurso que correspon de ao escopo da regra e há uma alteração na configuração do recurso. A avaliação é executada após o AWS Config envio de uma notificação de alteração do item de configura ção. Você escolhe quais recursos acionam a avaliação, definindo o escopo da regra. O escopo pode incluir o seguinte: • Um ou mais tipos de recursos • A combinação de um tipo de recurso e um ID de recurso

Tipo de gatilho	Descrição
	• A combinação de uma chave de tag e valor • Quando os recursos registrados são criados, atualizados ou excluídos AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponda ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações.
Periódico	AWS Config executa avaliações para a regra na frequência que você escolher; por exemplo, a cada 24 horas.
Híbrida	Algumas regras têm alterações na configura ção e gatilhos periódicos. Para essas regras, AWS Config avalia seus recursos quando detecta uma alteração na configuração e também na frequência que você especifica.

Modos de avaliação

Há dois modos de avaliação das AWS Config regras.

Modo de avaliação	Descrição
Proativo	Use a avaliação proativa para avaliar os recursos antes de serem implantados. Isso permite avaliar se um conjunto de proprieda des de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

Modo de avaliação	Descrição
	Para obter mais informações, consulte Modos de avaliação. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.
Detecção	Use a avaliação de detecção para avaliar os recursos que já foram implantados. Isso permite avaliar as definições de configuração de seus recursos existentes.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Gerenciando recursos excluídos com AWS Config regras lambda personalizadas

Os relatórios de regras sobre recursos excluídos devem retornar o resultado da avaliação de `NOT_APPLICABLE`, a fim de evitar avaliações desnecessárias de regras.

Quando você exclui um recurso, AWS Config cria um `configurationItem` com `ResourceDeleted` para `configurationItemStatus` o. Você pode usar esses metadados para verificar se uma regra relata sobre um recurso excluído. Para obter mais informações sobre itens de configuração, consulte Conceitos | Itens de configuração.

Inclua os seguintes trechos de código para verificar se há recursos excluídos e definir o resultado da avaliação de uma regra lambda AWS Config personalizada como `NOT_APPLICABLE` se ela reportasse sobre um recurso excluído:

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
```

```
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config as regras gerenciadas e as regras de política AWS Config personalizadas lidam com esse comportamento por padrão.
> Se você criar uma regra lambd AWS Config personalizada com Python usando AWS Config o Development Kit (RDK) AWS Config e a Development Kit Library (RDKlib), a classe Evaluator importada verificará esse comportamento. Para obter informações sobre como escrever regras com o RDK e o RDKlib, consulte Writing rules with the RDK and RDKlib.

Tópicos

- Criação AWS Config de regras de política personalizadas
- Creating (Criando)AWS ConfigRegras personalizadas do Lambda

Criação AWS Config de regras de política personalizadas

Você pode criar regras de política AWS Config personalizada a partir da AWS Config API AWS Management Console AWS CLI, ou. Para obter mais informações sobre como escrever regras com o Guard, consulte Escrevendo regras do Guard no Guia do usuário do AWS CloudFormation Guard. Para obter mais informações sobre os esquemas dos tipos de recursos suportados que AWS Config podem ser avaliados, consulte tipos de recursos no Resource Schema Repository. AWS Config GitHub

> **Important**
>
> O esquema AWS Config de recursos para avaliar itens de configuração é diferente do esquema CFN para avaliar modelos. AWS CloudFormation Se você usar o esquema CFN para regras de política personalizadas do AWS Config , os resultados da avaliação retornarão `NOT_APPLICABLE`. Use o esquema AWS Config de recursos ao criar regras de política AWS Config personalizada e escrever políticas com base na estrutura do item de configuração. Para obter uma lista de esquemas de AWS Config recursos, consulte tipos de recursos no Repositório de esquemas de recursos. AWS Config GitHub

Criação de regras de política AWS Config personalizadas (console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma AWS região que ofereça suporte a AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras).
4. Na página Rules (Regras), selecione Add rule (Adicionar regra).
5. Na página Especificar tipo de regra, escolha Criar regra personalizada usando o Guard.
6. Na página Configurar regra, configure a regra através das seguintes etapas:
   a. Para Nome, digite um nome exclusivo para a regra.
   b. Em Descrição, digite uma descrição para a regra.

c. Para a versão de tempo de execução do Guard, escolha o sistema de tempo de execução para sua regra de política AWS Config personalizada.

d. Para o Conteúdo da regra, você pode preenchê-lo com a política personalizada do Guard para sua regra. Para obter mais informações sobre a estrutura e os recursos das políticas personalizadas do Guard, consulte os Modos de operação do AWS CloudFormation Guard 2.0 no GitHub repositório do Guard.

> **Note**
>
> O esquema AWS Config de recursos para avaliar itens de configuração é diferente do esquema CFN para avaliar modelos. AWS CloudFormation Se você usar o esquema CFN para regras de política personalizadas do AWS Config , os resultados da avaliação retornarão `NOT_APPLICABLE`. Use o esquema AWS Config de recursos ao criar regras de política AWS Config personalizada e escrever políticas com base na estrutura do item de configuração. Para obter uma lista de esquemas AWS Config de recursos, consulte tipos de recursos no Repositório de esquemas de recursos. AWS Config GitHub

O exemplo a seguir mostra a definição da política para uma versão da regra de política AWS Config personalizada da regra AWS Config gerenciada. dynamodb-pitr-enabled

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription
        %pitr == "ENABLED"
}
```

e. No Modo de avaliação, escolha quando, no processo de criação e gerenciamento de recursos, você AWS Config deseja avaliar seus recursos. Dependendo da regra, AWS Config você pode avaliar suas configurações de recursos antes de um recurso ter sido provisionado, depois de um recurso ter sido provisionado, ou ambos.

   i. Escolha Ativar a avaliação proativa para permitir que você execute avaliações nas configurações de seus recursos antes de serem implantados.

      Depois de ativar a avaliação proativa, você pode usar a API de StartResourceavaliação e a GetResourceEvaluationSummaryAPI para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região.

      Para obter mais informações sobre como usar esses comandos, consulte Avaliando seus recursos com AWS Config regras. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

   ii. Escolha Ativar a avaliação de detecção para avaliar as definições de configuração de seus recursos existentes.

      Para avaliação de detetives, as regras de política AWS Config personalizada são iniciadas pelas alterações de configuração. Essa opção será pré-selecionada.

      - Recursos: quando um recurso que corresponde ao tipo de recurso especificado, ou ao tipo mais identificador, é criado, alterado ou excluído.
      - Tags: quando um recurso com a tag especificada é criado, alterado ou excluído.
      - Todas as alterações — Quando um recurso registrado por AWS Config é criado, alterado ou excluído.

      AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponde ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações. Caso contrário, as avaliações serão iniciadas quando houver uma alteração em um recurso pós-provisionado.

f. Para Parâmetros, você poderá personalizar os valores das chaves fornecidas, se sua regra incluir parâmetros. Um parâmetro é um atributo que seus recursos devem ter antes de serem considerados compatíveis com a regra.

7. Na página Revisar e criar, revise todas as suas seleções antes de adicionar a regra à sua Conta da AWS.
8. Ao terminar de revisar suas regras, escolha Adicionar regra.

Criação AWS Config de regras de política personalizadas (AWS CLI)

Use o comando `put-config-rule`.

O campo `Owner` deveria ser `CUSTOM_POLICY`. Os seguintes campos adicionais são obrigatórios para regras de política AWS Config personalizada:

- `Runtime`: o sistema de tempo de execução para suas regras de política AWS Config personalizada.
- `PolicyText`: a definição da política que contém a lógica para suas regras de política personalizadas do AWS Config .
- `EnableDebugLogDelivery`: a expressão booleana para ativar o registro de depuração para sua regra de política AWS Config personalizada. O valor padrão é `false`.

Criação de regras de política AWS Config personalizadas (API)

Use a ação PutConfigRegra.

O campo `Owner` deveria ser `CUSTOM_POLICY`. Os seguintes campos adicionais são obrigatórios para regras de política AWS Config personalizada:

- `Runtime`: o sistema de tempo de execução para suas regras de política AWS Config personalizada.
- `PolicyText`: a definição da política que contém a lógica para suas regras de política personalizadas do AWS Config .
- `EnableDebugLogDelivery`: a expressão booleana para ativar o registro de depuração para sua regra de política AWS Config personalizada. O valor padrão é `false`.

Creating (Criando)AWS ConfigRegras personalizadas do Lambda

Você pode desenvolver regras personalizadas e adicioná-las aAWS ConfigcomAWS Lambdafunções de da. Você associa cada regra personalizada a uma função Lambda, que contém a lógica que avalia se suaAWSos recursos estão em conformidade com a regra. Você associa essa função com

a sua regra, e a regra chama a função em resposta a alterações de configuração ou periodicamente. A função avalia se seus recursos são compatíveis com sua regra e envia os resultados da avaliação para AWS Config.

O exemplo emRegras personalizadas do Lambda (exemplo do Amazon EC2)orienta você na criação de uma regra Lambda personalizada pela primeira vez que avalia se cada uma de suas instâncias do EC2 é do tipo t2.micro. Ele inclui um exemplo de função do Lambda que você pode adicionar àAWS Lambdasem modificação. O exemplo emRegras personalizadas do Lambda (exemplo geral)fornece um exemplo mais geral para criar uma regra Lambda personalizada.

Para saber comoAWS Lambdafunções funcionam e como desenvolvê-las, veja oAWS LambdaGuia do desenvolvedor do.

Tópicos

- Regras personalizadas do Lambda (exemplo do Amazon EC2)
- Regras personalizadas do Lambda (exemplo geral)
- Exemplos de funções e eventos do AWS Lambda para regras do AWS Config

Regras personalizadas do Lambda (exemplo do Amazon EC2)

Esse procedimento orienta você no processo de criação de uma regra personalizada do Lambda que avalia se cada uma de suas instâncias do EC2 é do tipo t2.micro. AWS Config executará avaliações baseadas em eventos para essa regra, o que significa que ela verificará as configurações da sua instância sempre que AWS Config detectar uma alteração na configuração em uma instância. AWS Config sinalizará as instâncias t2.micro como compatíveis e todas as outras instâncias como não compatíveis. O status de compatibilidade será exibido no console AWS Config .

Para obter o melhor resultado com esse procedimento, você deve ter uma ou mais instâncias do EC2 em seu Conta da AWS. Suas instâncias devem incluir uma combinação de pelo menos uma instância t2.micro e outros tipos.

Para criar essa regra, primeiro você criará uma AWS Lambda função personalizando um blueprint no AWS Lambda console. Em seguida, você criará uma regra personalizada do Lambda em AWS Config e associará a regra à função.

Tópicos

- Criar uma função AWS Lambda para uma regra de configuração personalizada
- Criação de uma regra Lambda personalizada para avaliar instâncias do Amazon EC2

Criar uma função AWS Lambda para uma regra de configuração personalizada

1. Faça login no AWS Management Console e abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. No AWS Lambda console, escolha Criar uma função Lambda.
4. Selecione Use o esquema. Na barra de pesquisa, digite config-rule-change-triggered. Selecione o esquema nos resultados do filtro e escolha Configurar.
5. Na página Configure triggers (Configurar triggers), selecione Next (Próximo).
6. Na página Basic information, execute as etapas a seguir:
   a. Em Nome da função, insira **`InstanceTypeCheck`**.
   b. Em Função de execução, escolha Criar nova função nos modelos de AWS política.
   c. Para Runtime (Tempo de execução), mantenha Node.js.
   d. Para Nome da função, digite um nome.
   e. Em Modelos de política, selecione Permissões de regras do AWS Config .
   f. Para função de código da função do Lambda, mantenha o código pré-configurado. O código Node.js para a função é fornecido no editor de código. Para esse procedimento, você não precisa alterar o código.
   g. Verifique os detalhes e escolha Criar função. O AWS Lambda console exibe sua função.
7. Para verificar se a sua função está configurada corretamente, teste-a com as seguintes etapas:
   a. Escolha Teste no menu abaixo Visão geral da função e, em seguida, escolha Configurar evento de teste.
   b. Em Modelo, escolha Notificação de alteração de item de configuração do AWS Config .
   c. Em Nome, digite um nome.
   d. Escolha Testar. AWS Lambda testa sua função com o evento de exemplo. Se a sua função estiver funcionando como esperado, uma mensagem de erro semelhante à seguinte aparecerá em Execution result (Resultado de execução):

```
{
  "errorType": "InvalidResultTokenException,"
  "errorMessage": "Result Token provided is invalid",
```

```
. . .
```

Isso `InvalidResultTokenException` é esperado porque sua função é executada com êxito somente quando recebe um token de resultado de AWS Config. O token de resultado identifica a regra do AWS Config e o evento que causou a avaliação, e associa uma avaliação a uma regra. Essa exceção indica que sua função tem a permissão de que precisa para enviar resultados para o AWS Config. Caso contrário, a seguinte mensagem de erro será exibida: `not authorized to perform: config:PutEvaluations`. Se esse erro ocorrer, atualize a função que você atribuiu para sua função, para permitir a ação `config:PutEvaluations` e testar sua função novamente.

Criação de uma regra Lambda personalizada para avaliar instâncias do Amazon EC2

1. Abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido para a mesma região na qual você criou a AWS Lambda função para sua regra personalizada do Lambda.
3. Na página Rules (Regras), selecione Add rule (Adicionar regra).
4. Na página Especificar tipo de regra, escolha Criar regra personalizada.
5. Na página Configure rule (Configurar regra), conclua as seguintes etapas:
   a. Para Name (Nome), digite **`InstanceTypesAreT2micro`**.
   b. Em Description (Descrição), digite **`Evaluates whether EC2 instances are the t2.micro type`**.
   c. Em AWS Lambda function ARN, especifique o ARN que o AWS Lambda atribuiu à sua função.

      > **Note**
      > O ARN que você especificou nesta etapa não deve incluir o qualifier `$LATEST`. Você pode especificar um ARN sem um qualificador de versão ou com qualquer outro qualificador. `$LATEST` AWS Lambda oferece suporte ao controle de versão de funções, e cada versão recebe um ARN com um qualificador. AWS Lambda usa o `$LATEST` qualificador para a versão mais recente.

   d. Para Tipo de gatilho, escolha Quando a configuração muda.

e. Para Scope of changes (Escopo das alterações), escolha Resources (Recursos).

f. Em Recursos, escolha Instância do EC2 da AWS na lista suspensa Tipo de recurso.

g. Na seção Parâmetros, você deve especificar o parâmetro de regra que sua AWS Lambda função avalia e o valor desejado. A função para esse procedimento avalia o parâmetro `desiredInstanceType`.

   Em Key (Chave), digite **`desiredInstanceType`**. Em Value, digite **`t2.micro`**.

6. Escolha Próximo. Em Revisar página, verifique os detalhes da função e selecione Criar função. Sua nova regra aparece na página Rules (Regras).

   A conformidade exibirá Avaliação... até AWS Config receber os resultados da avaliação de sua AWS Lambda função. Se a regra e a função estiverem funcionando como esperado, um resumo dos resultados será exibido depois de alguns minutos. Por exemplo, um resultado de 2 noncompliant resource(s) (2 recursos não compatíveis) indica que duas de suas instâncias não são instâncias t2.micro, e um resultado de Compliant (Compatível) indica que todas as instâncias são t2.micro. Você pode atualizar os resultados com o botão de atualizar.

   Se a regra ou a função não funcionar como esperado, você pode consultar uma das opções abaixo para Compliance (Compatibilidade):

   - Nenhum resultado relatado - AWS Config avaliou seus recursos de acordo com a regra. A regra não se aplicou aos recursos da AWS em seu escopo, os recursos especificados foram excluídos, ou os resultados da avaliação foram excluídos. Para obter resultados de avaliação, atualize a regra, mude seu escopo ou selecione Re-evaluate (Reavaliar).

     Verifique se o escopo inclui Instância do AWS EC2 para Recursos e tente novamente.

   - Nenhum recurso no escopo - AWS Config não é possível avaliar seus AWS recursos registrados em relação a essa regra porque nenhum de seus recursos está dentro do escopo da regra. Para obter os resultados da avaliação, edite a regra e altere seu escopo ou adicione recursos AWS Config para registrar usando a página Configurações.

     Verifique se AWS Config está gravando instâncias do EC2.

   - Evaluations failed (Falha nas avaliações) – para obter informações que possam ajudar a determinar o problema, selecione o nome da regra para abrir sua página de detalhes e ver a mensagem de erro.

Se sua regra funcionar corretamente e AWS Config fornecer resultados de avaliação, você poderá saber quais condições afetam o status de conformidade de sua regra. Você pode saber quais recursos não são compatíveis e por quê. Para ter mais informações, consulte Visualizando informações de conformidade e resultados da avaliação.

Regras personalizadas do Lambda (exemplo geral)

Efetue o procedimento a seguir para criar uma regra personalizada do Lambda. Para criar uma regra personalizada do Lambda, primeiro você cria uma AWS Lambda função que contém a lógica de avaliação da regra. Em seguida, associe a função a uma regra personalizada do Lambda criada no AWS Config.

> **Important**
>
> Como prática recomendada de segurança ao permitir a AWS Config permissão para invocar sua função do Lambda, recomendamos fortemente que você restrinja o acesso à política baseada em recursos do `sourceARN` Lambda `sourceAccountId` com e/ou na solicitação de invocação. Para ter mais informações, consulte Prática recomendada de segurança para a política baseada em recursos do AWS Lambda.

Sumário

- Criar uma função AWS Lambda para uma regra de configuração personalizada
- Criando uma regra personalizada em AWS Config
- Prática recomendada de segurança para a política baseada em recursos do AWS Lambda
- Avaliar tipos de recursos adicionais

Criar uma função AWS Lambda para uma regra de configuração personalizada

Uma função Lambda é um código personalizado para AWS Lambda o qual você carrega e é invocado por eventos que são publicados nela por uma fonte de eventos. Se a função Lambda estiver associada a uma regra Config, ela será AWS Config invocada quando o gatilho da regra ocorrer. A função do Lambda avalia as informações de configuração enviadas pelo AWS Config e retorna os resultados da avaliação. Para mais informações sobre as funções do Lambda, consulte Origens de eventos e funções no Guia do desenvolvedor do AWS Lambda .

Você pode usar uma linguagem de programação compatível com AWS Lambda para criar uma função Lambda para uma regra Lambda personalizada. Para facilitar essa tarefa, você pode

personalizar um AWS Lambda blueprint ou reutilizar uma função de amostra do repositório de AWS Config regras GitHub.

Esquemas do AWS Lambda

O AWS Lambda console fornece exemplos de funções, ou esquemas, que você pode personalizar adicionando sua própria lógica de avaliação. Quando você cria uma função, você pode escolher um dos seguintes esquemas:

- config-rule-change-triggered— Acionado quando suas configurações AWS de recursos são alteradas.
- config-rule-periodic— Acionado na frequência que você escolher (por exemplo, a cada 24 horas).

AWS Config GitHub Repositório de regras

Um repositório público de exemplos de funções para regras personalizadas do Lambda está disponível GitHub no, um serviço de hospedagem e compartilhamento de código baseado na web. As funções de amostra são desenvolvidas e contribuídas pela AWS comunidade. Se quiser usar uma amostra, você pode copiar seu código em uma nova AWS Lambda função. Para exibir o repositório, consulte https://github.com/awslabs/aws-config-rules/.

Para criar a função para sua regra personalizada

1. Faça login no AWS Management Console e abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Escolha Create a Lambda function.
4. Na página Usar um blueprint, você pode escolher uma das funções do blueprint para AWS Config regras como ponto de partida ou pode continuar sem um blueprint escolhendo Ignorar.
5. Na página Configure triggers (Configurar triggers), selecione Next (Próximo).
6. Na página Informações básicas, digite um nome e uma descrição.
7. Em Runtime (Tempo de execução), escolha a linguagem de programação em que sua função foi criada.
8. Em Code entry type (Tipo de entrada de código), selecione o tipo de entrada desejada. Se você estiver usando um esquema, mantenha o código pré-configurado.

9. Forneça seu código usando o método exigido pelo tipo de entrada de código que você selecionou. Se estiver usando um esquema, o código da função é fornecido no editor de código, e você pode personalizá-lo para incluir sua própria avaliação lógica. Seu código pode avaliar os dados do evento AWS Config fornecidos quando invoca sua função:
   - Para funções baseadas no config-rule-change-triggeredblueprint ou para funções acionadas por alterações de configuração, os dados do evento são o item de configuração ou um objeto de item de configuração superdimensionado para o AWS recurso que foi alterado.
   - Para funções baseadas no config-rule-periodicblueprint ou para funções acionadas na frequência que você escolher, os dados do evento são um objeto JSON que inclui informações sobre quando a avaliação foi acionada.
   - Para os dois tipos de funções, AWS Config passa parâmetros de regra no formato JSON. Você pode definir quais parâmetros de regra são informados ao criar a regra personalizada no AWS Config.
   - Por exemplo, eventos que AWS Config são publicados quando invoca sua função, consulte. Eventos de exemplo para regras AWS Config
10. Para Função de execução, escolha Criar uma nova função com base em modelos de política da AWS .
11. Para Role name, digite um nome.
12. Para Policy templates, selecione AWS Config Rules permission.
13. Verifique os detalhes e escolha Criar função.

Criando uma regra personalizada em AWS Config

Use AWS Config para criar uma regra Lambda personalizada e associar a regra a uma função Lambda.

Para criar uma regra personalizada

1. Abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido para a mesma região na qual você criou a AWS Lambda função para sua regra personalizada do Lambda.
3. Na página Rules (Regras), selecione Add rule (Adicionar regra).
4. Na página Especificar tipo de regra, escolha Criar regra personalizada.

5. Na página Configure rule (Configurar regra), digite um nome e descrição.
6. Em AWS Lambda function ARN, especifique o ARN que o AWS Lambda atribuiu à sua função.

> **Note**
>
> O ARN que você especificou nesta etapa não deve incluir o qualifier `$LATEST`. Você pode especificar um ARN sem um qualificador de versão ou com qualquer outro qualificador. `$LATEST` AWS Lambda oferece suporte ao controle de versão de funções, e cada versão recebe um ARN com um qualificador. AWS Lambda usa o `$LATEST` qualificador para a versão mais recente.

7. Para Trigger type (Tipo de trigger), selecione uma ou ambas as opções abaixo:
   - Alterações de configuração — AWS Config invoca sua função Lambda quando detecta uma alteração na configuração.
   - Periódico — AWS Config invoca sua função Lambda na frequência que você escolher (por exemplo, a cada 24 horas).
8. Se os tipos de gatilho da sua regra incluírem alterações de configuração, especifique uma das seguintes opções para Escopo de alterações com o qual AWS Config invoca sua função Lambda:
   - Todas as alterações — Quando qualquer recurso registrado por AWS Config é criado, alterado ou excluído.
   - Recursos: quando um recurso que corresponde ao tipo especificado, ou ao tipo mais o identificador, é criado, alterado ou excluído.
   - Tags: quando um recurso com a tag especificada é criado, alterado ou excluído
9. Se os tipos de gatilho da sua regra incluírem Periódico, especifique a frequência com a qual AWS Config invoca sua função Lambda.
10. Na seção Parâmetros, especifique todos os parâmetros de regra que sua AWS Lambda função avalia e o valor desejado.
11. Escolha Próximo. Em Revisar página, verifique os detalhes da função e selecione Criar função. Sua nova regra aparece na página Regras.

    A conformidade exibirá Avaliação... até AWS Config receber os resultados da avaliação de sua AWS Lambda função. Se a regra e a função estiverem funcionando como esperado, um resumo

dos resultados será exibido depois de alguns minutos. Você pode atualizar os resultados com o botão de atualizar.

Se a regra ou a função não funcionar como esperado, você pode consultar uma das opções abaixo para Compliance (Compatibilidade):

- Nenhum resultado relatado - AWS Config avaliou seus recursos de acordo com a regra. A regra não se aplicou aos recursos da AWS em seu escopo, os recursos especificados foram excluídos, ou os resultados da avaliação foram excluídos. Para obter resultados de avaliação, atualize a regra, mude seu escopo ou selecione Re-evaluate (Reavaliar).

  Essa mensagem também podem aparecer se a regra não relatar resultados de avaliação.
- Sem recursos no escopo - AWS Config não é possível avaliar seus AWS recursos registrados em relação a essa regra porque nenhum de seus recursos está dentro do escopo da regra. Você pode escolher na página AWS Config Settings quais recursos o registrará.
- Evaluations failed (Falha nas avaliações) – para obter informações que possam ajudar a determinar o problema, selecione o nome da regra para abrir sua página de detalhes e ver a mensagem de erro.

> **Note**
>
> Quando você cria uma regra personalizada do Lambda com o AWS Config console, as permissões apropriadas são criadas automaticamente para você. Se você criar uma regra personalizada do Lambda com o AWS CLI, precisará dar AWS Config permissão para invocar sua função do Lambda usando o comando. `aws lambda add-permission` Para obter mais informações, consulte Usando políticas baseadas em recursos para (políticas de funções AWS Lambda Lambda) no Guia do desenvolvedor.AWS Lambda
> Antes de dar AWS Config permissão para invocar sua função Lambda, consulte a seção a seguir. Prática recomendada de segurança para a política baseada em recursos do AWS Lambda

Prática recomendada de segurança para a política baseada em recursos do AWS Lambda

Como prática recomendada de segurança, para evitar dar permissão de invocação para que todo o nome da entidade principal do serviço (SPN) chame sua função do Lambda, recomendamos

muito que você restrinja o acesso à política baseada em recursos do Lambda com `sourceARN` e/ou `sourceAccountId` na solicitação de invocação.

`sourceARN`É o ARN da AWS Config regra que está invocando a função Lambda.

O `sourceAccountId` é o ID da conta do usuário que criou a regra.

Restringir o acesso na política baseada em recursos do Lambda ajuda a AWS Lambda garantir que você esteja acessando seus recursos somente em nome dos usuários e cenários esperados.

Para adicionar permissão baseada em SPN, você precisa usar a seguinte CLI

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

Para adicionar permissão SourceAccountId baseada

Antes de a regra ser criada, é possível adicionar permissão baseada no `sourceAccountId` à política baseada em recursos com a CLI a seguir

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

Para adicionar ambas as permissões SourceArn e SourceAccountId com base

Depois que a regra for criada, você poderá adicionar a permissão baseada em `sourceARN` à política baseada em recursos com a seguinte CLI. Isso permite que somente um ARN de regra específico invoque a função do Lambda.

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

Avaliar tipos de recursos adicionais

Você pode criar regras personalizadas do Lambda para executar avaliações de tipos de recursos ainda não registrados pelo. AWS Config Isso é útil se você quiser avaliar a conformidade de tipos de recursos adicionais que AWS Config não são registrados atualmente. Para obter uma lista de tipos

de recursos adicionais que você pode avaliar com regras personalizadas, consulte AWS Resource Types Reference.

> **Note**
>
> Ao criar um Lambda personalizado para um tipo de recurso que não é registrado por AWS Config, a regra deve ter o tipo de gatilho periódico. O tipo de gatilho de alterações de configuração não é suportado. Para ter mais informações, consulte Modo de avaliação e tipos de gatilho para AWS Config regras.

Exemplo

1. Você deseja avaliar cofres do Amazon S3 Glacier em sua conta. Os recursos de cofre do Amazon S3 Glacier atualmente não são registrados pelo AWS Config.
2. Você cria uma AWS Lambda função que avalia se os cofres do Amazon S3 Glacier estão em conformidade com os requisitos da sua conta.
3. Você cria uma regra personalizada do Lambda chamada evaluate-glacier-vaultse, em seguida, atribui sua AWS Lambda função à regra.
4. AWS Config invoca sua função Lambda e, em seguida, avalia os cofres do Amazon S3 Glacier em relação à sua regra.
5. AWS Config retorna as avaliações e você pode ver os resultados de conformidade da sua regra.

> **Note**
>
> Você pode ver os detalhes da configuração na AWS Config linha do tempo e pesquisar recursos no AWS Config console em busca de recursos AWS Config compatíveis. Se você tiver configurado AWS Config para registrar todos os tipos de recursos, os recursos recém-suportados serão gravados automaticamente. Para ter mais informações, consulte Tipos de recursos compatíveis.

Exemplos de funções e eventos do AWS Lambda para regras do AWS Config

Cada regra personalizada do Lambda está associada a um Lambdafunção, que é um código personalizado que contém a lógica de avaliação da regra. Quando o gatilho de uma regra de Config

ocorre (por exemplo, quandoAWS Configdetecta uma alteração de configuração),AWS Configinvoca a função Lambda da regra publicando umevento, que é um objeto JSON que fornece os dados de configuração que a função avalia.

Para obter mais informações sobre funções e eventos emAWS Lambda, consulteFontes de funções e eventosnaAWS LambdaGuia do desenvolvedor do.

Tópicos

- Exemplo de AWS Lambda funções para AWS Config regras (Node.js)
- Exemplos de funções do AWS Lambda para regras do AWS Config (Python)
- Eventos de exemplo para regras AWS Config

Exemplo de AWS Lambda funções para AWS Config regras (Node.js)

AWS Lambda executa funções em resposta a eventos publicados pelos AWS serviços. A função de uma regra AWS Config personalizada do Lambda recebe um evento publicado por e AWS Config, em seguida, usa os dados que recebe do evento e recupera da AWS Config API para avaliar a conformidade da regra. As operações em uma função para uma regra Config diferem conforme a avaliação seja acionada por alterações de configuração ou acionada periodicamente.

Para obter informações sobre padrões comuns nas AWS Lambda funções, consulte Modelo de programação no Guia do AWS Lambda desenvolvedor.

Sumário

- Exemplo de função para avaliações acionadas por alterações de configuração
- Exemplo de função para avaliações periódicas

Exemplo de função para avaliações acionadas por alterações de configuração

AWS Config invocará uma função como o exemplo a seguir ao detectar uma alteração na configuração de um recurso que esteja dentro do escopo de uma regra personalizada.

Se você usar o AWS Config console para criar uma regra associada a uma função como este exemplo, escolha Alterações de configuração como o tipo de acionador. Se você usar a AWS Config API ou AWS CLI criar a regra, defina o `MessageType` atributo `ConfigurationItemChangeNotification` como `OversizedConfigurationItemChangeNotification` e. Essas configurações permitem que

sua regra seja acionada sempre que AWS Config gerar um item de configuração ou um item de configuração superdimensionado como resultado de uma alteração de recurso.

Este exemplo avalia seus recursos e verifica se as instâncias correspondem ao tipo de recurso `AWS::EC2::Instance`. A regra é acionada quando o AWS Config gera um item de configuração ou uma notificação de item de configuração superdimensionado.

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );
```

```
}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) =>
 {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}
```

```
// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches
 the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
```

```
                annotation = "This is an annotation describing why the resource is not
 compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

Operações de função

A função executa as seguintes operações em tempo de execução:

1. A função é executada quando AWS Lambda passa o `event` objeto para a `handler` função. Neste exemplo, a função aceita o `callback` parâmetro opcional, que ela usa para retornar informações ao chamador. AWS Lambda também passa um `context` objeto, que contém informações e métodos que a função pode usar enquanto é executada. Observe que nas versões mais recentes do Lambda, o contexto não é mais usado.

2. A função verifica se `messageType` para o evento é um item de configuração ou um item de configuração superdimensionado, e, em seguida, retorna o item de configuração.
3. O handler chama a função `isApplicable` para determinar se o recurso foi excluído.

> **Note**
>
> Os relatórios de regras sobre recursos excluídos devem retornar o resultado da avaliação de `NOT_APPLICABLE`, a fim de evitar avaliações desnecessárias de regras.

4. O manipulador chama a `evaluateChangeNotificationCompliance` função e passa os `ruleParameters` objetos `configurationItem` e AWS Config publicados no evento.

   A função primeiro avalia se o recurso é uma instância EC2. Se o recurso não é uma instância EC2, a função retorna um valor de compatibilidade de `NOT_APPLICABLE`.

   Em seguida, a função avalia se o atributo `instanceType` no item de configuração é igual ao valor de parâmetro `desiredInstanceType`. Se os valores são iguais, a função retornará `COMPLIANT`. Se os valores não são iguais, a função retornará `NON_COMPLIANT`.
5. O manipulador se prepara para enviar os resultados da avaliação AWS Config inicializando o objeto. `putEvaluationsRequest` Este objeto inclui o parâmetro `Evaluations`, que identifica o resultado de compatibilidade, o tipo de recurso e o ID do recurso que foi avaliado. O `putEvaluationsRequest` objeto também inclui o token de resultado do evento, que identifica a regra e o evento para AWS Config.
6. O manipulador envia os resultados da avaliação AWS Config passando o objeto para o `putEvaluations` método do `config` cliente.

Exemplo de função para avaliações periódicas

AWS Config invocará uma função como o exemplo a seguir para avaliações periódicas. As avaliações periódicas ocorrem com a frequência que você especifica ao definir a regra em AWS Config.

Se você usar o AWS Config console para criar uma regra associada a uma função como este exemplo, escolha Periódico como o tipo de acionador. Se você usar a AWS Config API ou criar AWS CLI a regra, defina o `MessageType` atributo como`ScheduledNotification`.

Este exemplo verifica se o número total de um recurso especificado excede o máximo especificado.

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount, count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
```

```
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
```

```
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource type.",
 null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

Operações de função

A função executa as seguintes operações em tempo de execução:

1. A função é executada quando AWS Lambda passa o `event` objeto para a `handler` função. Neste exemplo, a função aceita o `callback` parâmetro opcional, que ela usa para retornar

informações ao chamador. AWS Lambda também passa um `context` objeto, que contém informações e métodos que a função pode usar enquanto é executada. Observe que nas versões mais recentes do Lambda, o contexto não é mais usado.

2. Para contar os recursos do tipo especificado, o handler chama a função `countResourceTypes` e passa o parâmetro `applicableResourceType` que recebeu do evento. A função `countResourceTypes` chama o método `listDiscoveredResources` do cliente `config`, que retorna uma lista de identificadores para os recursos aplicáveis. A função usa o comprimento da lista para determinar o número de recursos aplicáveis e retorna essa contagem para o handler.
3. O manipulador se prepara para enviar os resultados da avaliação AWS Config inicializando o objeto. `putEvaluationsRequest` Esse objeto inclui o `Evaluations` parâmetro, que identifica o resultado da conformidade e o Conta da AWS que foi publicado no evento. Você pode usar o parâmetro `Evaluations` para aplicar o resultado a qualquer tipo de recurso que tenha suporte no AWS Config. O `putEvaluationsRequest` objeto também inclui o token de resultado do evento, que identifica a regra e o evento para AWS Config.
4. Dentro do objeto `putEvaluationsRequest`, o handler chama a função `evaluateCompliance`. Esta função testa se o número de recursos aplicáveis excede o máximo atribuído ao parâmetro `maxCount`, que foi fornecido pelo evento. Se o número de recursos excede o máximo, a função retorna `NON_COMPLIANT`. Se o número de recursos não excede o máximo, a função retorna `COMPLIANT`.
5. O manipulador envia os resultados da avaliação AWS Config passando o objeto para o `putEvaluations` método do `config` cliente.

Exemplos de funções do AWS Lambda para regras do AWS Config (Python)

O AWS Lambda executa funções em resposta a eventos publicados por serviços da AWS. A função para uma regra de lambda personalizada do AWS Config recebe um evento que é publicado pelo AWS Config. Em seguida, a função usa dados recebidos do evento, que foram recuperados da API do AWS Config, para avaliar a conformidade da regra. As operações em uma função para uma regra Config diferem conforme a avaliação seja acionada por alterações de configuração ou acionada periodicamente.

Para obter mais informações sobre padrões comuns nas funções do AWS Lambda, consulte Modelo de programação no Guia do desenvolvedor doAWS Lambda.

Sumário

- Exemplo de função para avaliações acionadas por alterações de configuração

- Exemplo de função para avaliações periódicas

Exemplo de função para avaliações acionadas por alterações de configuração

O AWS Config chamará uma função como a do exemplo a seguir, quando detectar a alteração de configuração de um recurso dentro do escopo de uma regra personalizada.

Se você usar o console do AWS Config para criar uma regra que esteja associada a uma função, como neste exemplo, escolha Configuration changes (Alterações da configuração) como o tipo de trigger. Se você usar a API do AWS Config ou a AWS CLI para criar a regra, defina o atributo `MessageType` para `ConfigurationItemChangeNotification` e `OversizedConfigurationItemChangeNotification`. Essas configurações habilitam sua regra para ser acionada sempre que o AWS Config gerar um item de configuração ou um item de configuração superdimensionado como resultado de uma mudança de recurso.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
```

```
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
```

```
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'], 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')
```

```
    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

Operações de função

A função executa as seguintes operações em tempo de execução:

1. A função é executada quando o AWS Lambda passa o objeto `event` para a função `handler`. Neste exemplo, a função aceita o parâmetro `callback` opcional, que ela usa para retornar informações para o chamador. O AWS Lambda também informa um objeto de `context`, que contém informações e métodos que a função pode usar enquanto é executada. Observe que nas versões mais recentes do Lambda, o contexto não é mais usado.
2. A função verifica se `messageType` para o evento é um item de configuração ou um item de configuração superdimensionado, e, em seguida, retorna o item de configuração.
3. O handler chama a função `isApplicable` para determinar se o recurso foi excluído.

> **Note**
>
> Os relatórios de regras sobre recursos excluídos devem retornar o resultado da avaliação de `NOT_APPLICABLE`, a fim de evitar avaliações desnecessárias de regras.

4. O manipulador chama a função `evaluateChangeNotificationCompliance` e transmite os objetos `configurationItem` e `ruleParameters` e que o AWS Config publicou no evento.

   A função primeiro avalia se o recurso é uma instância EC2. Se o recurso não é uma instância EC2, a função retorna um valor de compatibilidade de `NOT_APPLICABLE`.

   Em seguida, a função avalia se o atributo `instanceType` no item de configuração é igual ao valor de parâmetro `desiredInstanceType`. Se os valores são iguais, a função retornará `COMPLIANT`. Se os valores não são iguais, a função retornará `NON_COMPLIANT`.
5. O manipulador prepara o envio dos resultados da avaliação para o AWS Config, inicializando o objeto `putEvaluationsRequest`. Este objeto inclui o parâmetro `Evaluations`, que identifica o resultado de compatibilidade, o tipo de recurso e o ID do recurso que foi avaliado. O objeto `putEvaluationsRequest` também inclui o token de resultado do evento, que identifica a regra e o evento para o AWS Config.
6. O manipulador envia os resultados da avaliação para o AWS Config, transmitindo o objeto para o método `putEvaluations` do cliente `config`.

Exemplo de função para avaliações periódicas

O AWS Config chamará uma função como a do exemplo a seguir para avaliações periódicas. As avaliações periódicas ocorrem com a frequência que você especifica ao definir a regra em AWS Config.

Se você usar o console do AWS Config para criar uma regra que esteja associada a uma função, como neste exemplo, escolha Periodic (Periódico) como o tipo de trigger. Se você usar a API do AWS Config ou a AWS CLI para criar a regra, defina o atributo `MessageType` como `ScheduledNotification`.

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
```

```
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to
 the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on
 the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
```

```
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

Operações de função

A função executa as seguintes operações em tempo de execução:

1. A função é executada quando o AWS Lambda passa o objeto `event` para a função `handler`. Neste exemplo, a função aceita o parâmetro `callback` opcional, que ela usa para retornar informações para o chamador. O AWS Lambda também informa um objeto de `context`, que contém informações e métodos que a função pode usar enquanto é executada. Observe que nas versões mais recentes do Lambda, o contexto não é mais usado.
2. Para contar os recursos do tipo especificado, o handler chama a função `countResourceTypes` e passa o parâmetro `applicableResourceType` que recebeu do evento. A função `countResourceTypes` chama o método `listDiscoveredResources` do cliente `config`, que retorna uma lista de identificadores para os recursos aplicáveis. A função usa o comprimento da lista para determinar o número de recursos aplicáveis e retorna essa contagem para o handler.
3. O manipulador prepara o envio dos resultados da avaliação para o AWS Config, inicializando o objeto `putEvaluationsRequest`. Este objeto inclui o parâmetro `Evaluations`, que identifica o resultado da conformidade e a Conta da AWS que foi publicada no evento. Você pode usar o parâmetro `Evaluations` para aplicar o resultado a qualquer tipo de recurso que tenha suporte no AWS Config. O objeto `putEvaluationsRequest` também inclui o token de resultado do evento, que identifica a regra e o evento para o AWS Config.
4. Dentro do objeto `putEvaluationsRequest`, o handler chama a função `evaluateCompliance`. Esta função testa se o número de recursos aplicáveis excede o máximo atribuído ao parâmetro `maxCount`, que foi fornecido pelo evento. Se o número de recursos excede o máximo, a função retorna `NON_COMPLIANT`. Se o número de recursos não excede o máximo, a função retorna `COMPLIANT`.
5. O manipulador envia os resultados da avaliação para o AWS Config, transmitindo o objeto para o método `putEvaluations` do cliente `config`.

Eventos de exemplo para regras AWS Config

Quando o gatilho de uma regra ocorre, AWS Config invoca a AWS Lambda função da regra publicando um evento. Em seguida, AWS Lambda executa a função passando o evento para o manipulador da função.

Evento de exemplo para avaliações acionadas por alterações de configuração

AWS Config publica um evento quando detecta uma alteração na configuração de um recurso que está dentro do escopo de uma regra. O evento de exemplo a seguir mostra que a regra foi acionada por uma alteração de configuração para uma instância EC2.

```
{
```

```
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Evento de exemplo para avaliações acionadas por alterações de configuração superdimensionadas

Algumas alterações de recursos geram itens de configuração superdimensionados. O evento de exemplo a seguir mostra que a regra foi acionada por uma alteração de configuração superdimensionada para uma instância EC2.

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
```

```
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Evento de exemplo para avaliações acionadas por frequência periódica

AWS Config publica um evento quando avalia seus recursos na frequência especificada por você (como a cada 24 horas). O evento de exemplo a seguir mostra que a regra foi acionada por uma frequência periódica.

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion
\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Atributos do evento

O objeto JSON de um AWS Config evento contém os seguintes atributos:

`invokingEvent`

O evento que aciona a avaliação de uma regra. Se o evento é publicado em resposta a uma alteração de configuração de recursos, o valor para esse atributo é uma string que contém um arquivo JSON `configurationItem` ou um `configurationItemSummary` (para itens de configuração superdimensionados). O item de configuração representa o estado do recurso no momento em que AWS Config detectou a alteração. Para obter um exemplo de um item de

configuração, consulte a saída produzida pelo `get-resource-config-history` AWS CLI comando em[Visualizar o histórico de configuração](#).

Se o evento é publicado para uma avaliação periódica, o valor é uma string que contém um objeto JSON. O objeto inclui informações sobre a avaliação que foi acionada.

Para cada tipo de evento, uma função deve analisar a string com um analisador JSON para ser capaz de avaliar seu conteúdo, como mostrado no seguinte exemplo de Node.js:

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

Os pares de chave/valor que a função processa como parte de sua avaliação lógica. Você define parâmetros ao usar o AWS Config console para criar uma regra personalizada do Lambda. Você também pode definir parâmetros com o `InputParameters` atributo na solicitação `PutConfigRule` AWS Config da API ou no `put-config-rule` AWS CLI comando.

O código JSON para os parâmetros está contido em uma string, de modo que uma função deve analisar a string com um analisador JSON para ser capaz de avaliar seu conteúdo, como mostrado no seguinte exemplo de Node.js:

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

Um token para o qual a função deve passar AWS Config com a `PutEvaluations` chamada.

`eventLeftScope`

Um valor booleano que indica se o AWS recurso a ser avaliado foi removido do escopo da regra. Se o valor for `true`, a função indica que a avaliação pode ser ignorada especificando-se `NOT_APPLICABLE` como o valor para o atributo `ComplianceType` na chamada `PutEvaluations`.

`executionRoleArn`

O ARN da função do IAM atribuída a. AWS Config

`configRuleArn`

O ARN AWS Config atribuído à regra.

`configRuleName`

O nome que você atribuiu à regra que causou AWS Config a publicação do evento e a invocação da função.

`configRuleId`

O ID AWS Config atribuído à regra.

`accountId`

O ID do Conta da AWS proprietário da regra.

`version`

Um número de versão atribuído por AWS. A versão será incrementada se AWS adicionar atributos aos AWS Config eventos. Se uma função requer um atributo que está somente em eventos que correspondem ou excedem uma versão específica, essa função pode verificar o valor desse atributo.

A versão atual para AWS Config eventos é 1.0.

Adicionando, atualizando e excluindo regras AWS Config

Você pode usar o AWS Config console ou os AWS SDKs para visualizar, adicionar e excluir suas regras.

Adicionar, visualizar, atualizar e excluir regras (console)

A página Regras mostra as regras e os resultados atuais de conformidade na tabela. O resultado de cada regra é Avaliar... até AWS Config terminar de avaliar seus recursos de acordo com a regra. Você pode atualizar os resultados com o botão de atualizar. Ao AWS Config concluir as avaliações, você poderá ver as regras e os tipos de recursos que estão em conformidade ou não. Para ter mais informações, consulte Visualizando informações de conformidade e resultados da avaliação.

> **Note**
>
> AWS Config avalia somente os tipos de recursos que está gravando. Por exemplo, se você adicionar a regra habilitada para o cloudtrail, mas não registrar o tipo de recurso de CloudTrail trilha, não AWS Config poderá avaliar se as trilhas em sua conta estão em conformidade ou não. Para ter mais informações, consulte AWS Recursos de gravação.

Adicionar regras

Para adicionar uma regra

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras).
4. Na página Rules (Regras), selecione Add rule (Adicionar regra).
5. Na página Especificar tipo de regra, especifique o tipo de regra concluindo as seguintes etapas:
   a. Digitar no campo de pesquisa para filtrar a lista de regras gerenciadas por nome, descrição e rótulo da regra. Por exemplo, digite EC2 para retornar regras que avaliam tipos de recursos do EC2, ou digite periodic (periódico) para retornar regras que possuam trigger periódico.
   b. Você também pode criar sua própria regra. Escolha Criar regra personalizada usando Lambda ou Criar regra personalizada usando o Guard e siga o procedimento em Criação de regras personalizadas do AWS Config Lambda ou AWS Config Criação de regras de política personalizadas.
6. Na página Configurar regra, configure a regra através das seguintes etapas:
   a. Para Name (Nome), digite um nome exclusivo para a regra.
   b. Em Descrição, digite uma descrição para a regra.
   c. No Modo de avaliação, escolha quando, no processo de criação e gerenciamento de recursos, você AWS Config deseja avaliar seus recursos. Dependendo da regra, AWS Config pode avaliar suas configurações de recursos antes de um recurso ser implantado, depois de um recurso ter sido implantado ou ambos.
      i. Escolha Ativar a avaliação proativa para permitir que você execute avaliações nas configurações de seus recursos antes de serem implantados.

         Depois de ativar a avaliação proativa, você pode usar a API de StartResourceavaliação e a GetResourceEvaluationSummaryAPI para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região.

Para obter mais informações sobre como usar esses comandos, consulte Avaliando seus recursos com AWS Config regras. Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

ii. Escolha Ativar a avaliação de detecção para avaliar as definições de configuração de seus recursos existentes.

Para avaliação de detecção, existem dois tipos de gatilhos: Quando a configuração muda e Periódico.

A. Se os tipos de gatilho da sua regra incluírem alterações de configuração, especifique uma das seguintes opções para Escopo de alterações com o qual AWS Config invoca sua função Lambda:

- Recursos: quando um recurso que corresponde ao tipo de recurso especificado, ou ao tipo mais identificador, é criado, alterado ou excluído.
- Tags: quando um recurso com a tag especificada é criado, alterado ou excluído.
- Todas as alterações — Quando um recurso registrado por AWS Config é criado, alterado ou excluído.

AWS Config executa a avaliação quando detecta uma alteração em um recurso que corresponde ao escopo da regra. Você pode usar o escopo para restringir quais recursos iniciam as avaliações.

B. Se os tipos de gatilho da sua regra incluírem Periódico, especifique a frequência com a qual AWS Config invoca sua função Lambda.

d. Para Parâmetros, você poderá personalizar os valores das chaves fornecidas, se sua regra incluir parâmetros. Um parâmetro é um atributo que seus recursos devem ter antes de serem considerados compatíveis com a regra.

7. Na página Revisar e criar, revise todas as suas seleções antes de adicionar a regra à sua Conta da AWS. Se a regra ou a função não funcionar como esperado, você pode consultar uma das opções abaixo para Compatibilidade:

- Nenhum resultado relatado - AWS Config avaliou seus recursos de acordo com a regra. A regra não se aplicava aos AWS recursos em seu escopo, os recursos especificados foram excluídos ou os resultados da avaliação foram excluídos. Para obter resultados de avaliação, atualize a regra, mude seu escopo ou selecione Re-evaluate (Reavaliar).

Essa mensagem também podem aparecer se a regra não relatar resultados de avaliação.

- Nenhum recurso no escopo - AWS Config não é possível avaliar seus AWS recursos registrados em relação a essa regra porque nenhum de seus recursos está dentro do escopo da regra. Para obter os resultados da avaliação, edite a regra e altere seu escopo ou adicione recursos AWS Config para registrar usando a página Configurações.
- Evaluations failed (Falha nas avaliações) – para obter informações que possam ajudar a determinar o problema, selecione o nome da regra para abrir sua página de detalhes e ver a mensagem de erro.

Como visualizar regras

Para visualizar suas regras

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras).
4. A página Regras mostra todas as regras que estão atualmente em seu Conta da AWS. Ela lista o nome, a ação de correção associada e o status de conformidade de cada regra.
   - Escolha Add rule (Adicionar regra) para iniciar a criação de uma regra.
   - Escolha uma regra para ver suas configurações ou escolha uma regra e Exibir detalhes.
   - Consulte o status de compatibilidade da regra ao avaliar seus recursos.
   - Escolha uma regra e Editar regra para alterar as configurações da regra e definir uma ação de correção para uma regra não compatível.

Atualizar regras

Para atualizar uma regra

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.

2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras).
4. Escolha o ícone Editar regra para a regra que você deseja atualizar.
5. Modifique as configurações na página Editar regra para alterar a regra, conforme necessário.
6. Escolha Salvar.

Como excluir regras

Para excluir uma regra

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras).
4. Escolha uma regra da tabela que você deseja excluir.
5. Na lista suspensa Ações, escolha Excluir regra.
6. Quando solicitado, digite “Excluir” (diferencia maiúsculas de minúsculas) e escolha Excluir.

Como habilitar a avaliação proativa

Você pode usar a avaliação proativa para avaliar os recursos antes que eles sejam implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

O Esquema do tipo de recurso indica as propriedades de um recurso. Você pode encontrar o esquema do tipo de recurso em "extensões AWS públicas" no AWS CloudFormation registro ou com o seguinte comando da CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obter mais informações, consulte Gerenciamento de extensões por meio do AWS CloudFormation registro e da referência de tipos de AWS recursos e propriedades no Guia AWS CloudFormation do usuário.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Para ativar a avaliação proativa

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que ofereça suporte a AWS Config regras. Para obter a lista das regiões da AWS compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras). Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.
4. Escolha uma regra e, em seguida, escolha Editar regra para a regra que você deseja atualizar.
5. Para o Modo de avaliação, escolha Ativar a avaliação proativa para permitir que você execute avaliações nas definições de configuração de seus recursos antes de serem implantados.
6. Escolha Salvar.

Depois de ativar a avaliação proativa, você pode usar a API de StartResourceavaliação e a GetResourceEvaluationSummaryAPI para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região.

Por exemplo, comece com a StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",
```

```
 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Você deve receber o `ResourceEvaluationId` na saída:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Em seguida, use o `ResourceEvaluationId` com a GetResourceEvaluationSummary API para verificar o resultado da avaliação:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Você deve receber uma saída semelhante à seguinte:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver informações adicionais sobre o resultado da avaliação, como qual regra sinalizou um recurso como NON_COMPLIANT, use a API de recursos. GetCompliance DetailsBy

Exibir, atualizar ou adicionar e excluir regras (AWS SDKs)

Como visualizar regras

Os exemplos de códigos a seguir mostram como usar `DescribeConfigRules`.

CLI

AWS CLI

Para obter detalhes de uma regra AWS Config

O comando a seguir retorna detalhes de uma regra de AWS Config chamada: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Saída:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
```

```
}
```

- Para obter detalhes da API, consulte DescribeConfigRegras na Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo lista as regras de configuração da conta, com propriedades selecionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Saída:

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obter detalhes da API, consulte DescribeConfigRegras na referência de AWS Tools for PowerShell cmdlets.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- Para obter detalhes da API, consulte a Referência da API DescribeConfigRules in AWS SDK for Python (Boto3).

Atualizar ou adicionar regras

Os exemplos de códigos a seguir mostram como usar `PutConfigRule`.

CLI

AWS CLI

Para adicionar uma regra de Config AWS gerenciada

O comando a seguir fornece código JSON para adicionar uma regra Config AWS gerenciada:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` é um arquivo JSON que contém a configuração da regra:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para o `ComplianceResourceTypes` atributo, esse código JSON limita o escopo a recursos do `AWS::EC2::Instance` tipo, então o AWS Config avaliará somente instâncias do EC2 em relação à regra. Como a regra é uma regra gerenciada, o atributo `Owner` é definido como `AWS` e o atributo `SourceIdentifier` é definido como o identificador da regra, `REQUIRED_TAGS`.

Para o atributo `InputParameters`, as chaves de tag exigidas pela regra, `CostCenter` e `Owner` são especificados.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar a configuração da regra, execute o describe-config-rules comando e especifique o nome da regra.

Como adicionar uma regra do Config gerenciada pelo cliente

O seguinte comando fornece o código JSON para adicionar uma regra do Config gerenciada pelo cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` é um arquivo JSON que contém a configuração da regra:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para o `ComplianceResourceTypes` atributo, esse código JSON limita o escopo a recursos do `AWS::EC2::Instance` tipo, então o AWS Config avaliará somente instâncias do EC2 em

relação à regra. Como essa regra é uma regra gerenciada pelo cliente, o `Owner` atributo é definido como`CUSTOM_LAMBDA`, e o `SourceIdentifier` atributo é definido como o ARN da função Lambda AWS . O `SourceDetails` objeto é obrigatório. Os parâmetros especificados para o `InputParameters` atributo são passados para a função AWS Lambda quando o AWS Config a invoca para avaliar os recursos em relação à regra.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar a configuração da regra, execute o describe-config-rules comando e especifique o nome da regra.

- Para obter detalhes da API, consulte PutConfigRegra na Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.
```

```
        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Para obter detalhes da API, consulte Referência da API PutConfigRule in AWS SDK for Python (Boto3).

Como excluir regras

Os exemplos de códigos a seguir mostram como usar `DeleteConfigRule`.

CLI

AWS CLI

Para excluir uma regra de AWS Config

O comando a seguir exclui uma regra de AWS Config chamada: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Para obter detalhes da API, consulte DeleteConfigRegra na Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3)

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Para obter detalhes da API, consulte Referência da API DeleteConfigRule in AWS SDK for Python (Boto3).

Ativando a avaliação proativa ()AWS CLI

Você pode usar a avaliação proativa para avaliar os recursos antes que eles sejam implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

O Esquema do tipo de recurso indica as propriedades de um recurso. Você pode encontrar o esquema do tipo de recurso em "extensões AWS públicas" no AWS CloudFormation registro ou com o seguinte comando da CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obter mais informações, consulte Gerenciamento de extensões por meio do AWS CloudFormation registro e da referência de tipos de AWS recursos e propriedades no Guia AWS CloudFormation do usuário.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Para ativar a avaliação proativa

Use o comando `put-config-rule` e habilite `PROACTIVE` para`EvaluationModes`.

Depois de ativar a avaliação proativa, você pode usar o comando da CLI start-resource-evaluation e o comando da CLI get-resource-evaluation-summary para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região.

Por exemplo, comece com o comando start-resource-evaluation:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Você deve receber o `ResourceEvaluationId` na saída:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Em seguida, use `ResourceEvaluationId` com o get-resource-evaluation-summary para verificar o resultado da avaliação:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Você deve receber uma saída semelhante à seguinte:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver informações adicionais sobre o resultado da avaliação, como qual regra sinalizou um recurso como NON_COMPLIANT, use o comando da CLI get-compliance-details-by-resource.

> **Note**
>
> Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

Ativando a avaliação proativa (API)

Você pode usar a avaliação proativa para avaliar os recursos antes que eles sejam implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

O Esquema do tipo de recurso indica as propriedades de um recurso. Você pode encontrar o esquema do tipo de recurso em "extensões AWS públicas" no AWS CloudFormation registro ou com o seguinte comando da CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obter mais informações, consulte Gerenciamento de extensões por meio do AWS CloudFormation registro e da referência de tipos de AWS recursos e propriedades no Guia AWS CloudFormation do usuário.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Para ativar a avaliação proativa de uma regra

Use a ação PutConfigRegra e habilite `PROACTIVE` para`EvaluationModes`.

Depois de ativar a avaliação proativa, você pode usar a API de StartResourceavaliação e a GetResourceEvaluationSummaryAPI para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região. Por exemplo, comece com a StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
```

```
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Você deve receber o `ResourceEvaluationId` na saída:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Em seguida, use o `ResourceEvaluationId` com a GetResourceEvaluationSummary API para verificar o resultado da avaliação:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Você deve receber uma saída semelhante à seguinte:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver informações adicionais sobre o resultado da avaliação, como qual regra sinalizou um recurso como NON_COMPLIANT, use a API de recursos. GetCompliance DetailsBy

> **Note**
>
> Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.

Enviar avaliações de regras para o Security Hub

Depois de adicionar uma AWS Config regra, você também pode enviar avaliações de regras para AWS Security Hub. A integração entre o Security Hub AWS Config e o Security Hub permite que você faça a triagem e corrija as avaliações de regras junto com outras configurações incorretas e problemas de segurança.

Envie avaliações de regras para o Security Hub

Para enviar avaliações de regras para o Security Hub, você deve primeiro configurar AWS Security Hub e AWS Config, em seguida, adicionar pelo menos uma regra AWS Config gerenciada ou personalizada. Depois disso, começa AWS Config imediatamente a enviar avaliações de regras para o Security Hub. O Security Hub enriquece as avaliações de regras e as transforma em descobertas do Security Hub.

Para obter mais informações sobre essa integração, consulte Integrações AWS de serviços disponíveis no Guia do AWS Security Hub usuário.

Avaliando seus recursos com regras AWS Config

Quando você cria regras personalizadas ou usa regras gerenciadas, AWS Config avalia seus recursos em relação a essas regras. Você pode executar avaliações sob demanda para recursos em relação às suas regras. Por exemplo, isso é útil quando você cria uma regra personalizada e deseja verificar se AWS Config está avaliando corretamente seus recursos ou identificar se há algum problema com a lógica de avaliação da sua AWS Lambda função.

Exemplo

1. Você cria uma regra personalizada que avalia se os usuários do IAM; têm chaves de acesso ativas.
2. AWS Config avalia seus recursos em relação à sua regra personalizada.

3. Existe na sua conta um usuário do IAM; que não tem uma chave de acesso ativa. Sua regra não sinaliza corretamente esse recurso como NON_COMPLIANT.
4. Você corrige a regra e inicia a avaliação novamente.
5. Como você corrigiu a regra, ela avalia corretamente seus recursos e sinaliza o recurso de usuário do IAM; como NON_COMPLIANT.

Ao adicionar uma regra à sua conta, você pode especificar quando, no processo de criação e gerenciamento de recursos, você AWS Config deseja avaliar seus recursos. O processo de criação e gerenciamento de recursos é conhecido como provisionamento de recursos. Você escolhe o modo de avaliação para especificar quando, nesse processo, AWS Config deseja avaliar seus recursos.

Dependendo da regra, AWS Config você pode avaliar suas configurações de recursos antes de um recurso ser implantado, após a implantação de um recurso ou ambos. Avaliar um recurso antes que ele seja implantado é uma avaliação proativa. Avaliar um recurso após sua implantação é uma avaliação de detecção.

Modo proativo

Use a avaliação proativa para avaliar os recursos antes de serem implantados. Isso permite avaliar se um conjunto de propriedades de recursos, se usado para definir um AWS recurso, seria COMPATÍVEL ou NÃO COMPATÍVEL, considerando o conjunto de regras proativas que você tem em sua conta na sua região.

O Esquema do tipo de recurso indica as propriedades de um recurso. Você pode encontrar o esquema do tipo de recurso em "extensões AWS públicas" no AWS CloudFormation registro ou com o seguinte comando da CLI:

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

Para obter mais informações, consulte Gerenciamento de extensões por meio do AWS CloudFormation registro e da referência de tipos de AWS recursos e propriedades no Guia AWS CloudFormation do usuário.

> **Note**
>
> As regras proativas não corrigem os recursos marcados como NON_COMPLIANT nem impedem que eles sejam implantados.

Avaliar seus recursos

Para ativar a avaliação proativa

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que ofereça suporte a AWS Config regras. Para obter a lista das regiões da AWS compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. Na barra de navegação à esquerda, selecione Rules (Regras). Para obter uma lista de regras gerenciadas que oferecem suporte à avaliação proativa, consulte Lista de regras AWS Config gerenciadas por modo de avaliação.
4. Escolha uma regra e, em seguida, escolha Editar regra para a regra que você deseja atualizar.
5. Para o Modo de avaliação, escolha Ativar a avaliação proativa para permitir que você execute avaliações nas definições de configuração de seus recursos antes de serem implantados.
6. Escolha Salvar.

> **Note**
>
> Você também pode ativar a avaliação proativa usando o `put-config-rule`comando e habilitando `PROACTIVE` para `EvaluationModes` ou usando a PutConfigRuleação e habilitando `PROACTIVE` para`EvaluationModes`.

Depois de ativar a avaliação proativa, você pode usar a StartResourceEvaluationAPI e a GetResourceEvaluationSummaryAPI para verificar se os recursos especificados nesses comandos seriam sinalizados como NÃO COMPATÍVEIS pelas regras proativas da sua conta na sua região.

Por exemplo, comece com a StartResourceEvaluation API:

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

Você deve receber o `ResourceEvaluationId` na saída:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

Em seguida, use o `ResourceEvaluationId` com a GetResourceEvaluationSummary API para verificar o resultado da avaliação:

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

Você deve receber uma saída semelhante à seguinte:

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

Para ver informações adicionais sobre o resultado da avaliação, como qual regra sinalizou um recurso como NON_COMPLIANT, use a API. GetComplianceDetailsByResource

Modo de detecção

Use a avaliação de detecção para avaliar os recursos que já foram implantados. Isso permite avaliar as definições de configuração de seus recursos existentes.

Avaliar seus recursos (console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma região que suporte AWS Config regras. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.
3. No painel de navegação, escolha Rules. A página Regras mostra o nome, a ação de correção associada e o status de conformidade de cada regra.
4. Escolha uma regra na tabela.
5. Na lista suspensa Ações, escolha Reavaliar.
6. AWS Config começa a avaliar os recursos de acordo com sua regra.

> **Note**
>
> Você pode reavaliar uma regra uma vez a cada minuto. Você deve aguardar AWS Config a conclusão da avaliação de sua regra antes de iniciar outra avaliação. Você não pode executar uma avaliação se, ao mesmo tempo, a regra estiver sendo atualizada ou se a regra for excluída.

Avaliar seus recursos (CLI)

- Use o comando start-config-rules-evaluation:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName
```

AWS Config começa a avaliar as configurações de recursos registradas em relação à sua regra. Você também pode especificar várias regras em sua solicitação:

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

Avaliar seus recursos (API)

Use a ação StartConfigRulesEvaluation.

Excluindo resultados de avaliação das regras AWS Config

Depois de o AWS Config avaliar sua regra, você pode ver os resultados da avaliação na página Rules (Regras) ou na página Rules details (Detalhes das regras) para a regra. Se os resultados da avaliação estiverem incorretos ou se você quiser avaliar novamente, você pode excluir os resultados da avaliação atual para a regra. Por exemplo, se a regra estava avaliando incorretamente os seus recursos, ou você excluiu recursos recentemente da sua conta, pode excluir os resultados da avaliação e, em seguida, executar nova avaliação.

Excluindo resultados da avaliação (console)

1. Faça login no AWS Management Console e abra o console do AWS Config em https://console.aws.amazon.com/config/.
2. No AWS Management Console menu, verifique se o seletor de região está definido como uma AWS região que ofereça suporte a AWS Config regras. Para ver a lista de regiões suportadas, consulte AWS ConfigRegiões e endpoints no Referência geral da Amazon Web Services.
3. No painel de navegação, escolha Rules (Regras). A página Regras mostra o nome, a ação de remediação associada e o status de conformidade de cada regra.
4. Escolha uma regra da tabela.
5. Na lista suspensa Ações, escolha Excluir resultados.
6. Quando solicitado, digite Excluir (essa entrada diferencia maiúsculas de minúsculas) e escolha Excluir. Depois de excluir uma avaliação, você não poderá recuperá-la.
7. Depois que os resultados de avaliação são excluídos, você pode iniciar manualmente uma nova avaliação.

Excluindo resultados da avaliação (CLI)

- Use o comando delete-evaluation-results.

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

O AWS Config exclui os resultados da avaliação para a regra.

Excluindo resultados da avaliação (API)

Use a ação DeleteEvaluationResults.

Gerenciando AWS Config regras em todas as contas da sua organização

> **Important**
>
> As regras organizacionais podem ser criadas somente com o uso da API ou da CLI. Essa operação não é suportada no AWS Config console.

AWS Config permite que você gerencie AWS Config regras Contas da AWS em toda a organização. É possível:

- Crie, atualize e exclua AWS Config regras de forma centralizada em todas as contas da sua organização.
- Implante um conjunto comum de AWS Config regras em todas as contas e especifique contas nas quais AWS Config as regras não devem ser criadas.
- Use as APIs da conta de gerenciamento AWS Organizations para impor a governança, garantindo que as AWS Config regras subjacentes não possam ser modificadas pelas contas dos membros da sua organização.

Considerações

Para implantações em diferentes regiões

A chamada de API para implantar regras e pacotes de conformidade em todas as contas é AWS específica da região. No nível da organização, você precisa alterar o contexto da sua chamada de API para uma região diferente se quiser implantar regras em outras regiões. Por exemplo, para implantar uma regra no Leste dos EUA (Norte da Virgínia), altere a região para Leste dos EUA (Norte da Virgínia) e depois chame `PutOrganizationConfigRule`.

Para contas dentro de uma organização

Se uma nova conta entrar em uma organização, o pacote de regras ou conformidade será implantado nessa conta. Quando uma conta sai de uma organização, o pacote de regras ou conformidade é removido.

Se você implantar uma regra organizacional ou pacote de conformidade em uma conta de administrador da organização e, em seguida, estabelecer um administrador delegado e implantar uma regra organizacional ou pacote de conformidade na conta do administrador delegado, você não poderá ver a regra organizacional ou o pacote de conformidade na conta do administrador da organização a partir da conta do administrador delegado ou ver a regra organizacional ou o pacote de conformidade na conta do administrador delegado da conta do administrador da organização. As DescribeOrganizationConformancePacksAPIs DescribeOrganizationConfigRulese só podem ver e interagir com os recursos relacionados à organização que foram implantados de dentro da conta que chama essas APIs.

Mecanismo de repetição para novas contas adicionadas a uma organização

A implantação de regras organizacionais e pacotes de conformidade existentes só será repetida por sete horas após a adição de uma conta à sua organização se um gravador não estiver disponível. Espera-se que você crie um gravador, se não houver um dentro de sete horas após a adição de uma conta à sua organização.

Contas de gerenciamento da organização, administradores delegados e funções vinculadas a serviços

Se você estiver usando uma conta de gerenciamento da organização e pretende usar um administrador delegado para implantação organizacional, saiba que AWS Config não criará automaticamente a função vinculada ao serviço (SLR). Você deve criar manualmente a função vinculada ao serviço (SLR) separadamente usando o IAM.

Se você não tiver uma SLR para sua conta de gerenciamento, não poderá implantar recursos nessa conta a partir de uma conta de administrador delegado. Você ainda poderá implantar AWS Config regras nas contas dos membros a partir das contas de gerenciamento e de administrador delegado. Para obter mais informações, consulte Como usar funções vinculadas ao serviço no Guia do usuário AWS Identity and Access Management (IAM).

Implantação

Para obter informações sobre como integrar AWS Config com AWS Organizations, consulte AWS Config e AWS Organizations no Guia do AWS Organizations usuário. Certifique-se AWS Config de

que a gravação esteja ativada antes de usar as seguintes APIs para gerenciar AWS Config regras em toda a Contas da AWS organização:

- PutOrganizationConfigRule, adiciona ou atualiza a regra de configuração da organização para toda a organização, avaliando se seus AWS recursos estão em conformidade com as configurações desejadas.
- DescribeOrganizationConfigRules, retorna uma lista das regras de configuração da organização.
- GetOrganizationConfigRuleDetailedStatus, retorna o status detalhado de cada conta membro dentro de uma organização para uma determinada regra de configuração da organização.
- GetOrganizationCustomRulePolítica, retorna a definição da política contendo a lógica da regra de política personalizada de configuração da sua organização.
- DescribeOrganizationConfigRuleStatus, fornece o status de implantação da regra de configuração da organização para uma organização.
- DeleteOrganizationConfigRule, exclui a regra de configuração da organização especificada e todos os resultados da avaliação de todas as contas membros dessa organização.

Suporte regional

A implantação de AWS Config regras em contas de membros em uma AWS organização é suportada nas seguintes regiões.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (N. da	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Califórnia)			
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Correção de recursos não compatíveis com regras AWS Config

AWS Config permite corrigir recursos não compatíveis que são avaliados por. Regras do AWS Config AWS Config aplica a remediação usando documentos AWS Systems Manager de automação. Esses documentos definem as ações a serem executadas em AWS recursos não compatíveis avaliados por. Regras do AWS ConfigÉ possível associar documentos SSM usando o AWS Management Console ou usando APIs.

AWS Config fornece um conjunto de documentos de automação gerenciados com ações de remediação. Você também pode criar e associar documentos de automação personalizados às AWS Config regras.

Para aplicar remediação em recursos não compatíveis, você pode escolher a ação de remediação que deseja associar em uma lista pré-preenchida ou criar suas próprias ações de remediação personalizadas usando documentos SSM. AWS Config fornece uma lista recomendada de ações de remediação no AWS Management Console.

No AWS Management Console, você pode optar por remediar manualmente ou automaticamente os recursos não compatíveis associando ações de remediação às regras. AWS Config Com todas as ações de correção, é possível escolher a correção manual ou automática.

Tópicos

- Pré-requisito
- Configurar a correção manual (console)
- Configurar a correção automática (console)
- Excluir ação de correção (console)
- Gerenciar remediação (API)
- Suporte regional

Pré-requisito

Antes de começar a aplicar correções em recursos não compatíveis, é necessário selecionar uma regra e configurar a correção (manual ou automática) para ela.

Configurar a correção manual (console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Regras, à esquerda, e na página Regras selecione Adicionar regra para adicionar novas regras à lista de regras

   Para regras existentes, selecione a regra não compatível na lista de regras e escolha a lista suspensa Ações.
3. Na lista suspensa Ações, escolha Gerenciar correção. Selecione “Correção manual” e, em seguida, escolha a ação de correção apropriada na lista recomendada.

   > **Note**
   >
   > Você só pode gerenciar correções para regras não AWS Config vinculadas a serviços. Para obter mais informações, consulte Regras da AWS vinculadas ao serviço.

   Dependendo da ação de correção selecionada, serão exibidos parâmetros específicos ou não será exibido nenhum parâmetro.
4. (Opcional) Se quiser passar o ID de recurso dos recursos não compatíveis para a ação de correção, selecione Resource ID parameter (Parâmetro de ID do recurso). Se essa opção for selecionada, no tempo de execução, o parâmetro será substituído pelo ID do recurso a ser corrigido.

   Cada parâmetro tem um valor estático ou um valor dinâmico. Se não selecionar um parâmetro de ID do recurso específico na lista vertical, você poderá inserir valores para cada chave. Se você selecionar um parâmetro de ID da lista suspensa, você poderá inserir valores para todas as outras chaves, exceto para o parâmetro de ID do recurso selecionado.
5. Escolha Salvar. A página Rules (Regras) será exibida.

Para solucionar problemas de ações de remediação com falha, você pode executar o AWS comando da interface de linha de comando `describe-remediation-execution-status` para obter uma visão detalhada de uma execução de remediação para um conjunto de recursos. Os detalhes incluem estado, timestamps das etapas de execução de correção e quaisquer mensagens de erro referentes às etapas que falharam.

Configurar a correção automática (console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Regras, à esquerda, e na página Regras selecione Adicionar regra para adicionar novas regras à lista de regras.

   Para regras existentes, selecione a regra não compatível na lista de regras e escolha a lista suspensa Ações.
3. Na lista suspensa Ações, escolha Gerenciar correção. Selecione “Correção automática” e, em seguida, escolha a ação de correção apropriada na lista recomendada.

   > **Note**
   >
   > Você só pode gerenciar correções para regras não AWS Config vinculadas a serviços. Para obter mais informações, consulte Regras da AWS vinculadas ao serviço.

   Dependendo da ação de correção selecionada, serão exibidos parâmetros específicos ou não será exibido nenhum parâmetro.
4. Escolha Auto remediation (Correção automática) para corrigir automaticamente os recursos não compatíveis.

   Se um recurso ainda não estiver em conformidade após a correção automática, você poderá definir a regra para tentar a correção automática novamente. Insira as novas tentativas e os segundos desejados.

   > **Note**
   >
   > Há custos associados à execução de um script de correção várias vezes. As novas tentativas só ocorrem se a correção falhar e funcionar dentro do período especificado; por exemplo, cinco tentativas em 300 segundos.
5. (Opcional) Se quiser passar o ID de recurso dos recursos não compatíveis para a ação de correção, selecione Resource ID parameter (Parâmetro de ID do recurso). Se essa opção for selecionada, no tempo de execução, o parâmetro será substituído pelo ID do recurso a ser corrigido.

Cada parâmetro tem um valor estático ou um valor dinâmico. Se não selecionar um parâmetro de ID do recurso específico na lista vertical, você poderá inserir valores para cada chave. Se você selecionar um parâmetro de ID da lista suspensa, você poderá inserir valores para todas as outras chaves, exceto para o parâmetro de ID do recurso selecionado.

6. Escolha Salvar. A página Rules (Regras) será exibida.

Para solucionar problemas de ações de remediação com falha

Para solucionar problemas de ações de remediação com falha, você pode executar o AWS comando da interface de linha de comando `describe-remediation-execution-status` para obter uma visão detalhada de uma execução de remediação para um conjunto de recursos. Os detalhes incluem estado, timestamps das etapas de execução de correção e quaisquer mensagens de erro referentes às etapas que falharam.

A remediação automática pode ser iniciada até mesmo para recursos compatíveis

Se você ativar a correção automática para uma AWS Config regra específica usando a API de PutRemediationconfigurações ou o AWS Config console, ela iniciará o processo de correção para todos os recursos não compatíveis dessa regra específica. O processo de correção automática depende do instantâneo dos dados de conformidade, que é capturado periodicamente. Qualquer recurso não compatível que seja atualizado entre o cronograma de snapshots continuará sendo corrigido com base no último instantâneo de dados de conformidade conhecido.

Isso significa que, em alguns casos, a correção automática pode ser iniciada até mesmo para recursos compatíveis, já que o processador de bootstrap usa um banco de dados que pode ter resultados de avaliação obsoletos com base no último instantâneo de dados de conformidade conhecido.

Excluir ação de correção (console)

Para excluir uma regra, primeiro você deve excluir a ação de correção associada a essa regra.

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Regras à esquerda e na página Regras, selecione a regra na lista de regras e selecione Editar.
3. Na página *`nome da página da regra`*, vá para a seção Ação de correção. Expanda a seção para ver detalhes adicionais.

4. Na seção Ação de correção, escolha Excluir e confirme sua ação de exclusão.

> **Note**
>
> Se a correção estiver em andamento, a ação de correção não será excluída. Se você selecionar Excluir ação de correção, não será possível recuperar a ação de correção. A exclusão de uma ação de correção não exclui a regra associada.

Se uma ação de correção for excluída, o parâmetro ID do recurso ficará vazio e exibirá N/A. Na página Regras, a coluna da ação de correção exibirá Não definida para a regra associada.

Gerenciar remediação (API)

Correção manual

Use as seguintes ações de AWS Config API para gerenciar a remediação:

- DeleteRemediationConfiguração, exclui a configuração de remediação.
- DescribeRemediationConfigurações, retorna os detalhes de uma ou mais configurações de remediação.
- DescribeRemediationExecutionStatus, fornece uma visão detalhada de uma execução de remediação para um conjunto de recursos, incluindo estado, registros de data e hora de quando as etapas da execução da remediação ocorrem e quaisquer mensagens de erro das etapas que falharam.
- PutRemediationConfigura, adiciona ou atualiza a configuração de remediação com uma AWS Config regra específica com o alvo ou a ação selecionada.
- StartRemediationExecução, executa uma remediação sob demanda para as AWS Config regras especificadas em relação à última configuração de remediação conhecida.

Correção automática

Use as seguintes ações de AWS Config API para gerenciar a correção automática:

- PutRemediationExceções, adiciona uma nova exceção ou atualiza uma exceção existente para um recurso específico com uma regra específica AWS Config .
- DescribeRemediationExceções, retorna os detalhes de uma ou mais exceções de remediação.

- DeleteRemediationExceções, exclui uma ou mais exceções de remediação mencionadas nas chaves de recursos.

Suporte regional

Atualmente, as ações de remediação AWS Config das Regras são suportadas nas seguintes regiões:

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (N. da Califórnia)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
África (Cidade do Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo	
Ásia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
Ásia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milão)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Espanha)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurique)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Solução de problemas

Verifique os seguintes problemas para solucionar se você não conseguir excluir uma AWS Config regra ou receber um erro semelhante ao seguinte: “Ocorreu um erro com AWS Config”.

A entidade AWS Identity and Access Management (IAM) tem permissões para a DeleteConfigRule API

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários ou Funções.
3. Escolha o usuário ou a função que você usou para excluir a AWS Config regra e expanda as políticas de permissões.
4. Na guia Permissões, escolha JSON.
5. No painel de visualização do JSON, confirme se a política do IAM permite permissões para a API DeleteConfigRule.

O limite de permissão da entidade IAM permite a API DeleteConfigRule

Se a entidade do IAM tiver um limite de permissões, certifique-se de que ela permita permissões para a DeleteConfigRule API.

1. Abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Usuários ou Funções.
3. Escolha o usuário ou a função que você usou para excluir a AWS Config regra, expanda o limite de permissões e escolha JSON.
4. No painel de visualização do JSON, confirme se a política do IAM permite permissões para a API DeleteConfigRule.

> **Warning**
>
> Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

A política de controle de serviços (SCP) permite a API DeleteConfigRule

1. Abra o AWS Organizations console em https://console.aws.amazon.com/organizations/ usando a conta de gerenciamento da organização.
2. Em Nome da conta, escolha Conta da AWS o.
3. Em Políticas, expanda Políticas de controle de serviços e observe as políticas de SCP anexadas.
4. Na parte superior da página, escolha Políticas.

5. Selecione a política e, em seguida, escolha Exibir detalhes.
6. No painel de visualização do JSON, confirme se a política permite a API de DeleteConfigregras.

A regra não é uma regra vinculada a serviços

Quando você habilita um padrão de segurança, AWS Security Hub cria regras vinculadas a serviços para você. Você não pode excluir essas regras vinculadas ao serviço usando AWS Config, e o botão de exclusão está esmaecido. Para remover uma regra vinculada ao serviço, consulte Desabilitar um padrão de segurança no Guia do Usuário do Security Hub.

Nenhuma ação de remediação está em andamento

Você não pode excluir AWS Config regras que tenham ações de remediação em andamento. Siga as etapas para excluir a ação de remediação associada a essa regra. Em seguida, tente excluir a regra novamente.

> **Important**
>
> Exclua somente ações de remediação que estejam em estado de falha ou sucesso.

Pacotes de conformidade

Um pacote de conformidade é um conjunto de AWS Config regras e ações de remediação que podem ser facilmente implantadas como uma única entidade em uma conta e uma região ou em uma organização em. AWS Organizations

Os pacotes de conformidade são criados usando um modelo YAML criado por você que contenha a lista de regras gerenciadas ou personalizadas do AWS Config e as ações de correção. Você também pode usar AWS Systems Manager documentos (documentos SSM) para armazenar seus modelos de pacotes de conformidade AWS e implantar diretamente pacotes de conformidade usando nomes de documentos SSM. É possível implantar o modelo usando o console do AWS Config ou a AWS CLI.

Para começar rapidamente e avaliar seu AWS ambiente, use um dos exemplos de modelos de pacote de conformidade. Você também pode criar um arquivo YAML do pacote de conformidade do zero com base no Pacote de conformidade personalizado.

Tópicos

- Pré-requisitos
- Suporte regional
- AWS Config Verificações de processo em um pacote de conformidade
- Exemplos de modelos de pacote de conformidade
- Pacotes de conformidade personalizados
- Visualizar dados de conformidade no painel de controle dos pacotes de conformidade
- Visualizar o cronograma do histórico de conformidade dos pacotes de conformidade
- Implantar um pacote de conformidade usando o console do AWS Config
- Implantar um pacote de conformidade usando a AWS Command Line Interface
- Gerenciar pacotes de conformidade (API)
- Gerenciar pacotes de conformidade em todas as contas na organização
- Solução de problemas

Pré-requisitos

Antes de implantar seu pacote de conformidade, ative a gravação. AWS Config

Comece a AWS Config gravar

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configurações no painel de navegação.
3. Para iniciar a gravação, em Recording is off (A gravação está desativada), selecione Turn on (Ativar). Quando solicitado, escolha Continuar.

Pré-requisitos para usar um pacote de conformidade com correção

Antes de implantar pacotes de conformidade usando modelos de amostra com remediação, você deve criar recursos apropriados, como automação, assumir funções e outros AWS recursos com base em sua meta de remediação.

Se tiver uma função de automação existente que está usando para correção usando documentos SSM, você poderá fornecer diretamente o ARN dessa função. Se tiver recursos, você poderá fornecê-los no modelo.

> **Note**
>
> Ao implantar um pacote de conformidade com correção em uma organização, o ID da conta de gerenciamento da organização precisa ser especificado. Caso contrário, durante a implantação do pacote de conformidade organizacional, o AWS Config substituirá automaticamente o ID da conta de gerenciamento pelo ID da conta de membro.

AWS Config não oferece suporte a funções AWS CloudFormation intrínsecas para a função de execução de automação. É necessário fornecer o ARN exato da função como uma string.

Para obter mais informações sobre como passar o ARN exato, consulte Exemplos de modelos de pacote de conformidade. Ao usar modelos de exemplo, atualize o ID da sua conta e o ID da conta de gerenciamento da organização.

Pré-requisitos para usar um pacote de conformidade com uma ou mais regras AWS Config

Antes de implantar um pacote de conformidade com uma ou mais AWS Config regras personalizadas, crie recursos apropriados, como a AWS Lambda função e a função de execução correspondente.

Se você tiver uma AWS Config regra personalizada existente, poderá fornecer diretamente a AWS Lambda função ARN of para criar outra instância dessa regra personalizada como parte do pacote.

Se você não tiver uma AWS Config regra personalizada existente, poderá criar uma AWS Lambda função e usar o ARN da função Lambda. Para ter mais informações, consulte AWS Config Regras personalizadas.

Se sua AWS Lambda função estiver presente em outra Conta da AWS, você poderá criar AWS Config regras com a autorização apropriada da AWS Lambda função entre contas. Para obter mais informações, consulte Como gerenciar AWS Config regras de forma centralizada em várias postagens Contas da AWS do blog.

Same account bucket policy

AWS Config Para poder armazenar artefatos do pacote de conformidade, você precisará fornecer um bucket do Amazon S3 e adicionar as seguintes permissões. Para obter mais informações sobre como nomear seu bucket, consulte Regras de nomeação de bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
```

```
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config Para poder armazenar artefatos do pacote de conformidade, você precisará fornecer um bucket do Amazon S3 e adicionar as seguintes permissões. Para obter mais informações sobre como nomear seu bucket, consulte Regras de nomeação de bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
```

```
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> Ao implantar pacotes de conformidade entre contas, o nome do bucket Amazon S3 de entrega deve começar com `awsconfigconforms`.

Pré-requisitos para pacotes de conformidade da organização

Especifique um ARN de função de execução de automação para essa correção no modelo se o modelo de entrada tiver uma configuração de correção automática. Verifique se existe uma função com o nome especificado em todas as contas (gerenciamento e membro) de uma organização. Você deve criar essa função em todas as contas antes de chamar `PutOrganizationConformancePack`. Você pode criar essa função manualmente ou usando os AWS CloudFormation conjuntos de pilhas para criar essa função em todas as contas.

Se seu modelo usa uma função AWS CloudFormation intrínseca `Fn::ImportValue` para importar uma variável específica, essa variável deve ser definida como uma `Export Value` em todas as contas dos membros dessa organização.

Para AWS Config regras personalizadas, consulte Como gerenciar centralmente AWS Config as regras em vários Contas da AWS blogs para configurar as permissões adequadas.

Política de bucket da organização:

AWS Config Para poder armazenar artefatos do pacote de conformidade, você precisará fornecer um bucket do Amazon S3 e adicionar as seguintes permissões. Para obter mais informações sobre como nomear seu bucket, consulte Regras de nomeação de bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
```

```
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> Ao implantar pacotes de conformidade em uma organização, o nome do bucket do Amazon S3 de entrega deve começar com `awsconfigconforms`.

Suporte regional

Os pacotes de conformidade são compatíveis com as seguintes regiões:

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
(Norte da Virgínia)			
Oeste dos EUA (N. da Califórnia)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

A implantação de pacotes de conformidade nas contas dos membros de uma AWS organização é suportada nas seguintes regiões.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (N. da	us-west-1	config.us-west-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Califórnia)			
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config Verificações de processo em um pacote de conformidade

As verificações de processo são um tipo de AWS Config regra que permite rastrear suas tarefas externas e internas que exigem verificação como parte dos pacotes de conformidade. Essas verificações podem ser adicionadas a um pacote de conformidade existente ou a um novo pacote de conformidade. Você pode monitorar toda a conformidade, incluindo AWS Config prazos e verificações manuais, em um único local.

Com as verificações de processo, você pode listar a conformidade dos requisitos e ações em um único local. Essas verificações de processo ajudam a aumentar a cobertura dos pacotes de conformidade baseados em regimes de conformidade. Você pode expandir ainda mais o pacote de conformidade adicionando novas verificações de processo que rastreiam processos e ações que precisam de verificação e rastreamento manuais. Isso permite que o pacote de conformidade se torne o modelo que fornece detalhes sobre AWS Config prazos e processos manuais para um regime de conformidade.

Você pode rastrear e gerenciar a conformidade de processos não associados às alterações de configuração de recursos em um pacote de conformidade como verificações de processos. Por exemplo, você pode adicionar uma verificação de processo para rastrear o requisito de conformidade do PCI-DSS para armazenar o backup de mídia em um local externo. Você avaliará manualmente a conformidade disso de acordo com as diretrizes do PCI-DSS ou de acordo com as orientações da sua organização.

Disponibilidade regional: as verificações de processo com os pacotes de conformidade estão disponíveis em todos os Regiões da AWS lugares em que os pacotes de AWS Config conformidade estão disponíveis. Para ter mais informações, consulte Suporte regional.

Tópicos

- Exemplo de modelo de pacote de conformidade para criar verificações de processo
- Inclua verificações de processo em um pacote de conformidade
- Alterar o status de conformidade de uma verificação de processo
- Exibir e editar a verificação do processo (console)

Exemplo de modelo de pacote de conformidade para criar verificações de processo

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

Veja dois modelos de exemplo, o modelo Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1 e o modelo Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2 .

Inclua verificações de processo em um pacote de conformidade

1. Adicione uma verificação de processo no modelo do pacote de conformidade. Consulte o modelo de exemplo anterior.

   ```
   Resources:
     ConfigEnabledAllRegions:
       Properties:
         ConfigRuleName: Config-Enabled-All-Regions
         Description: Ensure AWS Config is enabled in all Regions.
         Source:
           Owner: AWS
           SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
       Type: AWS::Config::ConfigRule
   ```

2. Insira o nome da verificação do processo.
3. Insira a descrição da verificação do processo.

4. Implante o pacote de conformidade a partir do Console de Gerenciamento da AWS. Para ter mais informações, consulte Implantar um pacote de conformidade usando o console do AWS Config.

> **Note**
>
> Você também pode implantar pacotes de conformidade usando o Command Line Interface (AWS CLI). Para ter mais informações, consulte Implantar um pacote de conformidade usando a AWS Command Line Interface.

Alterar o status de conformidade de uma verificação de processo

Alterar o status de conformidade de uma verificação de processo (console)

Para alterar o status de conformidade de uma verificação de processo (Console)

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Navegue até a página AWS Config Regras.
3. Escolha o nome da verificação do processo que você especificou no modelo junto com o identificador no pacote de conformidade.

> **Note**
>
> Todas as verificações de processo do mesmo pacote de conformidade têm o mesmo sufixo.

4. Na página Detalhes da regra, você não pode editar a regra, mas pode editar a conformidade da regra. Na seção Conformidade manual, escolha Editar conformidade.
5. Escolha a conformidade apropriada na lista suspensa.
6. (Opcional) Insira uma descrição para o status de conformidade.
7. Escolha Salvar.

Alterar o status de conformidade de uma verificação de processo (CLI)

Para alterar o status de conformidade de uma verificação de processo (CLI)

Você pode atualizar a conformidade das verificações de processo em um pacote de conformidade usando o AWS Command Line Interface (AWS CLI).

Para instalar o AWS CLI em sua máquina local, consulte Instalação da AWS CLI no Guia do AWS CLI usuário.

Se necessário, digite `AWS Config ure` para configurar o AWS CLI para usar uma AWS região em que os pacotes de AWS Config conformidade estejam disponíveis.

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando a seguir para atualizar a conformidade de um processo`Account ID`, verifique onde `ComplianceResourceId` está seu e inclua o nome da sua regra.

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. Pressione Enter para executar o comando.

Alterar o status de conformidade de uma verificação de processo (API)

Para alterar o status de conformidade de uma verificação de processo (API)

Depois que a implantação for concluída, para atualizar as avaliações e a conformidade das verificações do processo, use a API `PutExternalEvaluation`. Para obter mais informações, consulte PutExternalAvaliação.

Exibir e editar a verificação do processo (console)

Você pode visualizar as verificações do processo somente depois que um estado de conformidade for adicionado às verificações do processo. Escolha o pacote de conformidade específico para visualizar todas as verificações de processo dentro desse pacote de conformidade. Aqui você pode ver uma lista de verificações de processo que estão em conformidade e não conformidade.

Como essa é uma regra vinculada ao serviço, você não pode editar a verificação do processo na página de detalhes da regra.

> **Note**
>
> No entanto, você pode atualizar a conformidade da verificação do processo escolhendo Editar conformidade e selecionando o valor apropriado entre Compatível, Não compatível ou Não aplicável.

Você pode editar ou excluir uma verificação de processo do pacote de conformidade em que você adicionou as verificações de processo.

Exemplos de modelos de pacote de conformidade

Aqui estão os modelos YAML do pacote de conformidade que você vê no console. AWS Config Em cada modelo de pacote de conformidade, é possível usar uma ou mais regras do AWS Config e ações de correção. As regras do AWS Config listadas no pacote de conformidade podem ser regras gerenciadas do AWS Config e/ou regras personalizadas do AWS Config. Você pode baixar todos os modelos de pacotes de conformidade em. GitHub

> **Important**
>
> Os pacotes de conformidade fornecem uma estrutura de trabalho de conformidade de uso geral para ajudar a criar verificações de governança de segurança, operacionais ou de otimização de custos usando regras gerenciadas ou personalizadas do AWS Config e ações de correção do AWS Config. Os modelos de exemplo de pacote de conformidade da AWS pretendem ajudar você a criar seus próprios pacotes de conformidade com regras diferentes ou adicionais, parâmetros de entrada e ações de correção adequadas ao seu ambiente. Os modelos de exemplo, incluindo aqueles relacionados a padrões de conformidade e benchmarks do setor, não foram projetados para garantir sua conformidade com um padrão de governança específico. Eles não podem substituir seus esforços internos nem garantir que você passará por uma avaliação de conformidade.

> **Note**
>
> É recomendável que você revise as regras disponíveis na região em que você implanta um pacote de conformidade (Lista de regras AWS Config gerenciadas por disponibilidade

regional) e altere o modelo das regras que ainda não estão disponíveis nessa região antes da implantação.

Tópicos

- AWSPacote de conformidade Control Tower Detective Guardrails
- Práticas operacionais recomendadas para workloads de materiais do CCIG 2.0 da ABS
- Práticas recomendadas operacionais para workloads padrão do CCIG da ABS 2.0
- Práticas recomendadas operacionais para o ACSC Essential 8
- Práticas recomendadas operacionais para o ISM do ACSC
- Práticas recomendadas operacionais para IA e ML
- Práticas recomendadas operacionais para o Amazon API Gateway
- Melhores práticas operacionais para a Amazon CloudWatch
- Melhores práticas operacionais para o Amazon DynamoDB
- Melhores práticas operacionais para o Amazon S3
- Práticas recomendadas operacionais do CPG 234 da APRA
- Práticas recomendadas operacionais para o gerenciamento de ativos
- Práticas recomendadas operacionais para o AWS Backup
- Melhores práticas operacionais para gerenciamento de AWS identidade e acesso
- Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework
- Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework
- Práticas recomendadas operacionais para BCP e DR
- Práticas recomendadas operacionais para o BNM RMit
- Práticas recomendadas operacionais para o perfil de controle de nuvem médio do Canadian Centre for Cyber Security (CCCS)
- Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1
- Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2
- Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG1
- Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG2
- Práticas recomendadas operacionais para CIS Critical Security Controls v8 IG3

- Práticas recomendadas operacionais para o CIS Top 20
- Prática recomendadas operacionais para o CISA Cyber Essentials
- Práticas recomendadas operacionais para Serviços de Informação da Justiça Criminal (CJIS)
- Práticas recomendadas operacionais para a CMMC Nível 1
- Práticas recomendadas operacionais para a CMMC Nível 2
- Práticas recomendadas operacionais para a CMMC Nível 3
- Práticas recomendadas operacionais para a CMMC Nível 4
- Práticas recomendadas operacionais para a CMMC Nível 5
- Práticas recomendadas operacionais para o CMMC 2.0 Nível 1
- Práticas recomendadas operacionais para a CMMC 2.0 Nível 2
- Práticas recomendadas operacionais para serviços de computação
- Práticas recomendadas operacionais para a resiliência de dados
- Práticas recomendadas operacionais para serviços de bancos de dados
- Práticas recomendadas operacionais para o data lakes e os serviços de análise
- Práticas recomendadas operacionais para o DevOps
- Práticas recomendadas operacionais para o EC2
- Práticas recomendadas operacionais para criptografia e gerenciamento de chaves
- Práticas recomendadas operacionais do Guia de segurança cibernética da ENISA para PMEs
- Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Low
- Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Medium
- Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) High
- Operational Best Practices for FDA Title 21 CFR Part 11
- Práticas recomendadas operacionais para o FedRAMP (Baixo)
- Operational Best Practices for FedRAMP(Moderate)
- Operational Best Practices for FFIEC
- Práticas recomendadas operacionais do Catálogo de Critérios de Conformidade de Computação em Nuvem da Alemanha (C5)
- Práticas recomendadas operacionais para o Gramm Leach Bliley Act (GLBA)
- Práticas recomendadas operacionais para o Anexo 11 da GxP da UE
- Operational Best Practices for HIPAA Security

- Práticas recomendadas operacionais para o IRS 1075
- Práticas recomendadas operacionais para o K-ISMS
- Práticas recomendadas operacionais para o balanceamento de carga
- Práticas recomendadas operacionais para o Registro
- Práticas recomendadas operacionais para serviços de gerenciamento e governança
- Práticas recomendadas operacionais para o Aviso 655 do MAS
- Práticas recomendadas operacionais para as TRMG da MAS
- Práticas recomendadas operacionais para o monitoramento
- Práticas recomendadas de operação para as TRMG do NBC
- Práticas recomendadas operacionais para o NERC CIP BCSI
- Práticas recomendadas operacionais para o NCSC Cloud Security Principles
- Práticas recomendadas operacionais para a Estrutura de Avaliação Cibernética do NCSC
- Práticas recomendadas operacionais para serviços de rede e entrega de conteúdo
- Práticas recomendadas operacionais para o NIST 800-53 rev 4
- Práticas recomendadas de operação do NIST 800-53 rev 5
- Práticas recomendadas operacionais do NIST 800 171
- Práticas recomendadas operacionais do NIST 800 172
- Práticas recomendadas operacionais do NIST 800 181
- Práticas recomendadas operacionais do NIST 1800 25
- Práticas recomendadas operacionais do NIST CSF
- Práticas recomendadas operacionais para o NIST Privacy Framework v1.0
- Práticas recomendadas operacionais para o NYDFS 23
- Práticas recomendadas operacionais para o CIS
- Práticas recomendadas operacionais para o PCI DSS 3.2.1
- Práticas recomendadas operacionais para recursos acessíveis ao público
- Práticas recomendadas operacionais para a estrutura de segurança cibernética do RBI para UCBs
- Práticas recomendadas operacionais para o RBI MD-ITF
- Práticas recomendadas operacionais para serviços de segurança, identidade e conformidade
- Práticas recomendadas operacionais para tecnologia sem servidor

- Práticas recomendadas operacionais para serviços de armazenamento
- Práticas recomendadas operacionais para SWIFT CSP
- Práticas recomendadas de segurança do Amazon Elastic Container Service (Amazon ECS)
- Práticas recomendadas de segurança do Amazon Elastic File System (Amazon EFS)
- Práticas recomendadas de segurança do Amazon Elastic Kubernetes Service (Amazon EKS)
- Melhores práticas de segurança para a Amazon CloudFront
- Melhores práticas de segurança para o Amazon OpenSearch Service
- Práticas recomendadas de segurança para o Amazon Redshift
- Práticas recomendadas de segurança do Amazon Relational Database Service (Amazon RDS)
- Práticas recomendadas de segurança do AWS Auto Scaling
- Práticas recomendadas de segurança do AWS CloudTrail
- Práticas recomendadas de segurança do AWS CodeBuild
- Práticas recomendadas de segurança para o Amazon ECR
- Práticas recomendadas de segurança do AWS Lambda
- Práticas recomendadas de segurança do AWS Network Firewall
- Melhores práticas de segurança para a Amazon SageMaker
- Práticas recomendadas de segurança do AWS Secrets Manager
- Práticas recomendadas de segurança do AWS WAF
- Modelos de exemplo com ação de correção

AWSPacote de conformidade Control Tower Detective Guardrails

O modelo está disponível em GitHub: AWSControl Tower Detective Guardrails Conformance Pack.

Práticas operacionais recomendadas para workloads de materiais do CCIG 2.0 da ABS

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é

responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Guia de Implementação de Computação em Nuvem do ABS 2.0 - Cargas de trabalho de materiais e regras de configuração AWS gerenciadas. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do Guia de Implementação de Computação em Nuvem do ABS. Um controle do Guia de implementação de computação em nuvem da ABS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and

ID de controle	AWS Regra de configuração	Orientação
		Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataActionObrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelec idos. Isso pode ajudar a definir o número de solicitações que a função atende em determina do momento.
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventári o das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacion al, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	As identidades e as credencias são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	As identidades e as credencias são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	As identidades e as credencias são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-material-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para cargas de trabalho de materiais do ABS CCIG 2.0.

Práticas recomendadas operacionais para workloads padrão do CCIG da ABS 2.0

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Guia de Implementação de Computação em Nuvem do ABS 2.0 - Cargas de trabalho padrão e regras de configuração AWS gerenciadas. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do Guia de Implementação de Computação em Nuvem do ABS. Um controle do Guia de implementação de computação em nuvem da ABS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
section4a-govern-the-cloud-3-standard-workloads	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	As identidades e as credencias são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained (verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para cargas de trabalho padrão ABS CCIG 2.0.

Práticas recomendadas operacionais para o ACSC Essential 8

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Modelo de Maturidade Essential Eight do Australian Cyber Security Centre (ACSC) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles ACSC Essential Eight. Um controle do Essential Eight do ACSC pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos. Alguns dos mapeamentos para regras de configuração são para a seção de ordem superior (por exemplo. Estratégias de mitigação para limitar a extensão dos incidentes de segurança cibernética), em oposição às seções mais prescritivas.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do ACSC Essential 8, que foi criado pela Commonwealth of Australia e pode ser encontrado no ACSC | Essential Eight. O licenciamento do framework sob a Licença Pública Internacional de Atribuição Creative Commons 4.0 e as informações sobre os direitos autorais da estrutura (incluindo uma isenção de garantias) podem ser encontradas em ACSC | Direitos autorais.

ID de controle	AWS Regra de configuração	Orientação
Application_control	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações

ID de controle	AWS Regra de configuração	Orientação
		web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
Application_control	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
Application_control	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
Application_control	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
Application_control	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	AWS Regra de configuração	Orientação
Application_control	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
Application_control	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
Patch_applications	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
Patch_applications	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Patch_applications	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.
Patch_applications	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
Patch_applications	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
Patch_applications	ec2-managedinstance-associa tion-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Syste ms Manager atribui um estado de configuração às instância s gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
Patch_applications	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).
Restrict_administrative_privileges	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.
Restrict_administrative_privileges	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, pois a autenticação é gerenciada externamente.
Restrict_administrative_privileges	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
Multi-factor_authentication	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Multi-factor_authentication	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
Multi-factor_authentication	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
Multi-factor_authentication	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
Multi-factor_authentication	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
Regular_backups	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Regular_backups	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
Regular_backups	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
Regular_backups	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnitConfig default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
Regular_backups	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Regular_backups	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o ACSC Essential 8.

Práticas recomendadas operacionais para o ISM do ACSC

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Manual de Segurança da Informação (ISM) 2020-06 do Australian Cyber Security Center (ACSC) e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles ISM. Um controle do ISM pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro da estrutura do ISM, que foi criada pela Comunidade da Austrália e pode ser encontrado no Manual de Segurança da Informação (ISM) do governo australiano. O licenciamento do framework sob a Licença Pública Internacional de Atribuição Creative Commons 4.0 e as informações sobre os direitos autorais da estrutura (incluindo uma isenção de garantias) podem ser encontradas em ACSC | Direitos autorais.

ID de controle	AWS Regra de configuração	Orientação
43	response-plan-exists-maintained (verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.
252	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
261	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
261	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro

ID de controle	AWS Regra de configuração	Orientação
		em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
261	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
298	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
298	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
298	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
298	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	AWS Regra de configuração	Orientação
380	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.
459	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
459	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
459	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
459	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
459	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
459	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
459	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
459	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
459	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
459	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
459	sagemaker-endpoint-configur ation-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
459	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
459	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
459	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
459	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.

ID de controle	AWS Regra de configuração	Orientação
459	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
459	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
459	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
459	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
459	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
580	audit-log-policy-exists (verifica ção do processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	AWS Regra de configuração	Orientação
634	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
859	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
974	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
974	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
1139	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefini das usadas para a negociaçã o SSL quando é estabelec ida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográ ficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptore s SSL. A política de segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1173	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
1173	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1173	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
1173	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
1173	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
1228	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
1240	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
1240	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
1271	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
1271	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
1277	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
1277	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente.
1277	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
1380	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
1380	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1380	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.
1380	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
1380	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
1380	ec2-managedinstance-associa tion-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Syste ms Manager atribui um estado de configuração às instância s gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
1380	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1380	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
1380	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
1380	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
1380	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	AWS Regra de configuração	Orientação
1380	ecs-containers-nonprivileged	Para ajudar na implement ação do princípio de privilégi o mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégi o elevado habilitado. Quando esse parâmetro é verdadeir o, o contêiner recebe privilégi os elevados na instância de contêiner host (semelhante ao usuário raiz).
1380	ecs-containers-readonly-acc ess	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
1380	ecs-task-definition-nonroot-user	Para ajudar na implement ação do princípio de privilégi o mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	AWS Regra de configuração	Orientação
1380	efs-access-point-enforce-user-identity	Para ajudar na implement ação do princípio de privilégi o mínimo, habilite a fiscaliza ção do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configura da no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.
1380	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
1380	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente.
1380	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
1380	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	AWS Regra de configuração	Orientação
1380	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1380	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1380	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
1388	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1388	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
1401	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
1401	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
1401	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
1401	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
1401	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1402	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
1404	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
1405	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
1405	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD _TRAIL_ENABLED
1405	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
1405	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1405	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
1405	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
1405	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
1405	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1405	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
1405	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
1405	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
1405	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
1405	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
1405	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.
1405	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
1405	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1490	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1490	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
1490	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
1490	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencion al.

ID de controle	AWS Regra de configuração	Orientação
1490	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
1490	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
1501	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
1504	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
1504	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
1504	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
1504	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
1504	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1509	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
1509	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
1509	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.
1509	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
1509	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1509	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
1509	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
1509	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
1509	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1509	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
1509	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
1509	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
1509	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
1509	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
1509	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.
1509	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
1509	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1511	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
1511	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1511	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
1511	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1511	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1511	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
1511	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1511	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.
1511	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
1511	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1511	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnitConfig default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
1511	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
1511	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1511	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1511	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
1511	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnitConfig default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
1511	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
1515	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
1515	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1515	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1515	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1515	elasticache-redis-cluster-automatic-backup-check	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
1515	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
1515	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
1515	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.
1515	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1515	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnitConfig default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
1515	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
1515	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
1515	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
1536	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
1537	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
1537	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1552	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
1552	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
1552	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
1552	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
1552	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
1579	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
1580	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
1580	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
1580	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitad a para auxiliar na disponibi lidade dos dados armazenad os. Cada zona de disponibi lidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
1650	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
1650	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
1650	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.
1650	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
1650	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1650	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
1650	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
1650	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
1650	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1650	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
1650	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
1650	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
1650	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
1650	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
1650	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.
1650	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
1650	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1657	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1657	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
1657	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1657	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
1657	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencion al.
1657	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	AWS Regra de configuração	Orientação
1657	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.
161	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
161	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
161	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.
161	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
161	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
161	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
161	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
161	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
161	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
161	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
161	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
161	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
161	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
161	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
1679	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
1679	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
1679	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
1679	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
1679	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1680	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
1680	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
1680	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
1680	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1680	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
1681	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
1681	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
1681	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
1681	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
1681	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1683	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
1683	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
1690	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
1690	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1690	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.
1690	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
1690	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
1690	ec2-managedinstance-associa tion-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Syste ms Manager atribui um estado de configuração às instância s gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
1690	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1691	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
1691	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1691	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.
1691	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
1691	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
1691	ec2-managedinstance-associa tion-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Syste ms Manager atribui um estado de configuração às instância s gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
1691	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1693	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
1693	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1693	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.
1693	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
1693	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
1693	ec2-managedinstance-associa tion-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Syste ms Manager atribui um estado de configuração às instância s gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
1693	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
1694	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
1695	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
1707	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	AWS Regra de configuração	Orientação
P1	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
P1	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
P3	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
P5	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
P7	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
P7	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
P7	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
P7	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
P8	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
P9	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
P9	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnitConfig default: days). O valor real deve refletir os requisitos da organização.
P9	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
P9	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
P9	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
P9	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
P9	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
P9	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
P9	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
P9	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
P9	elasticache-redis-cluster-automatic-backup-check	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
P9	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
P9	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
P9	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
P10	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
P10	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
P10	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
P10	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
P10	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
P11	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o ACSC ISM.

Práticas recomendadas operacionais para IA e ML

Esse pacote de conformidade contém AWS Config regras baseadas em IA e ML. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para IA e ML.

Práticas recomendadas operacionais para o Amazon API Gateway

Esse pacote de conformidade contém AWS Config regras baseadas no uso do Amazon API Gateway. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para o Amazon API Gateway.

Melhores práticas operacionais para a Amazon CloudWatch

Este pacote de conformidade contém AWS Config regras baseadas no uso interno da Amazon CloudWatch . AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para a Amazon CloudWatch.

Melhores práticas operacionais para o Amazon DynamoDB

O modelo está disponível em GitHub: Operational Best Practices for Amazon DynamoDB.

Melhores práticas operacionais para o Amazon S3

O modelo está disponível em GitHub: Melhores práticas operacionais para o Amazon S3.

Práticas recomendadas operacionais do CPG 234 da APRA

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é

responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o CPG 234 da Australian Prudential Regulation Authority (APRA) e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles APRA CPG 234. Um controle do CPG 234 da APRA pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro da estrutura do CPG 234 da APRA de 2019, que foi criado pela Comunidade da Austrália e que pode ser encontrado no Guia prático de gestão de riscos: Segurança da informação do CPG 234. O licenciamento da estrutura sob a Licença Pública Internacional de Atribuição Creative Commons 3.0 e as informações sobre os direitos autorais da estrutura (incluindo uma isenção de garantias) podem ser encontrados em APRA | Copyright.

ID de controle	AWS Regra de configuração	Orientação
36a	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
36a	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no

ID de controle	AWS Regra de configuração	Orientação
		inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.
36a	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
36b	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
36b	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
36b	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
36b	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
36b	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
36b	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
36b	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
36c	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
36c	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
36c	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
36c	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36c	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
36c	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
36c	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
36c	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
36c	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.

ID de controle	AWS Regra de configuração	Orientação
36d	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
36d	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
36d	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36d	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
36d	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36d	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
36d	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
36d	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
36d	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
36d	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
36d	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36d	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
36d	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
36d	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
36d	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
36d	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36d	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
36d	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
36d	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
36d	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
36d	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36d	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
36d	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
36d	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
36d	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.
36d	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
36d	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
36d	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.
36d	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
36d	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
36d	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
36d	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
36d	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	AWS Regra de configuração	Orientação
36d	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
36d	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
36d	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
36e	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	AWS Regra de configuração	Orientação
36e	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
36e	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
36e	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36e	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
36e	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
36e	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
36e	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
36e	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
36e	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
36e	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
36e	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
36e	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36e	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
36e	s3-bucket-public-read-prohi bited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
36e	s3-bucket-public-write-proh ibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
36e	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
36e	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
36e	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
36e	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
36e	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
36e	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
36e	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	AWS Regra de configuração	Orientação
36e	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
36e	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
36e	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
36e	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
36f	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36f	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
36f	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36f	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
36f	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36f	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
36f	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
36f	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
36f	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
36f	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
36f	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
36f	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
36f	s3-bucket-public-read-prohi bited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
36f	s3-bucket-public-write-proh ibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
36f	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
36f	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
36f	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
36f	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
36f	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
36f	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
36f	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
36f	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
36f	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
36f	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
36f	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
36f	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
36f	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
36f	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
36f	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
36g	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
36g	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
36g	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
36h	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
36h	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
36h	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
36h	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
36h	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
36h	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
36h	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36h	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
36i	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
36i	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
36i	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36i	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
36i	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelec idos. Isso pode ajudar a definir o número de solicitações que a função atende em determina do momento.
36i	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	AWS Regra de configuração	Orientação
36i	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
36i	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
36i	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
36i	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
36i	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
36j	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
36j	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
36j	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.
36j	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
36j	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
36j	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
36j	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
36j	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.
36j	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
36j	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
36j	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
36l	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.
36l	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
36l	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
36l	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
36l	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
36l	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
36l	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
36l	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
36l	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
36l	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
36l	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
36l	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
36l	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
36l	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
36l	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
36l	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.

ID de controle	AWS Regra de configuração	Orientação
39(a)(b)(d)	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
39(a)(b)(d)	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
39(a)(b)(d)	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
40	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
40	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
40	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
40	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
44a	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
44a	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
44a	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
44b	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
44b	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
44b	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
44c	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	AWS Regra de configuração	Orientação
44c	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
44c	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
44c	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
45	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
45	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
45	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
45	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
45	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
45	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
45	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
45	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
45	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
45	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
45	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
45	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
45	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
45	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
45	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
45	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
45	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
45	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
45	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
45	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
45	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
45	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
45	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
45	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
45	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
45	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
45	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
45	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
45	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
45	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
45	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.

ID de controle	AWS Regra de configuração	Orientação
45	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
45	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.
45	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
45	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
45	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
45	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
45	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
45	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
45	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
45	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
45	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
45	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
47c	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
47c	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
47c	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
47c	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
47c	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
47c	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
47c	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
52c	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
52c	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
52c	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
52c	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
52c	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .

ID de controle	AWS Regra de configuração	Orientação
52c	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
52c	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
52c	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
52c	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
52c	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
52c	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
52c	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
52c	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
52c	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
52c	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
52c	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
52c	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
52c	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
52d	s3-bucket-public-read-prohi bited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
52d	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
52d	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
52d	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
52d	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
52d	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
52d	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
52d	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
52d	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
52d	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
52d	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
52d	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
52d	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
52d	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
52d	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
52d	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
52d	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
52d	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
52d	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
52d	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
52d	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
52d	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
52d	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
52e	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
52e	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
53	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
53	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
53	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
53	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
53	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
53	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
53	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
53	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
53	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
53	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
53	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
53	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
53	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
53	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
53	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
53	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
53	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
53	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
53	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
53	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
53	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	AWS Regra de configuração	Orientação
53	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
53	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
54	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
54	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
54	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
54	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
54	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
54	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
54	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
54	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
54	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
54	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
54	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
54	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
54	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
54	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
54	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
54	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
54	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
54	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
54	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
54	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
54	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
54	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
54	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
54	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
54	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
54	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
55	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
55	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
67	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
67	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
67	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
67	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
67	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
67	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
67	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
67	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
67	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
67	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
67	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
67	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
67	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
67	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
67	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
67	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	AWS Regra de configuração	Orientação
67	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
67	elasticsearch-logs-to-cloud watch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
68	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
68	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
73	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
73	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentA_1(b)(h)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentA_1(b)(h)	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentA_1(b)(h)	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
AttachmentA_1(c)	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(c)	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AttachmentA_1(e)	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AttachmentA_1(e)	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
AttachmentA_1(e)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
AttachmentA_1(e)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
AttachmentA_1(e)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
AttachmentB_1	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
AttachmentC_4	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentC_4	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentC_4	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
AttachmentC_4	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
AttachmentC_4	root-account-hardware-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
AttachmentC_4	secretsmanager-rotation-ena bled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programaç ão regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AttachmentC_4	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.
AttachmentC_4	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_4	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AttachmentC_5	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_5	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AttachmentC_5	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_5	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_5	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
AttachmentC_6	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AttachmentC_6	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_6	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
AttachmentC_7(c)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
AttachmentC_7(h)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AttachmentC_7(h)	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
AttachmentC_7(h)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
AttachmentC_7(h)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(h)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
AttachmentC_7(h)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(i)	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
AttachmentC_7(j)	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(j)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
AttachmentC_7(j)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_7(j)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
AttachmentC_8	opensearch-logs-to-cloudwat ch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
AttachmentC_8	api-gw-execution-logging-en abled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AttachmentC_8	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
AttachmentC_8	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
AttachmentC_8	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
AttachmentC_8	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
AttachmentD_1	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
AttachmentD_1	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub
AttachmentE_4	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
AttachmentE_4	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_5(d)	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
AttachmentE_1(a)(b)(d)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AttachmentE_1(a)(b)(d)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AttachmentE_1(a)(b)(d)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o APRA CPG 234.

Práticas recomendadas operacionais para o gerenciamento de ativos

Este pacote de conformidade contém AWS Config regras baseadas no gerenciamento de ativos interno. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para gerenciamento de ativos.

Práticas recomendadas operacionais para o AWS Backup

Este pacote de conformidade contém AWS Config regras baseadas em. AWS Backup AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para AWS Backup.

Melhores práticas operacionais para gerenciamento de AWS identidade e acesso

O modelo está disponível em GitHub: Melhores práticas operacionais para gerenciamento de AWS identidade e acesso.

Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o pilar de confiabilidade do Well-Architected Framework da Amazon Web Services e as regras de configuração gerenciadas. AWS Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais dos princípios de design do pilar. Uma categoria do Well-Architected Framework pode estar relacionada a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-1	Como você gerencia cotas de serviço e restrições? Para arquiteturas de workload baseadas em nuvem, existem cotas de serviço (que também são chamadas de limites de serviço). Essas	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	cotas existem para evitar o provision amento acidental de mais recursos do que você precisa e para limitar as taxas de solicitaç ão nas operações de API, a fim de proteger os serviços contra uso abusivo. Também há restrições de recursos, por exemplo, a taxa em que você pode propagar bits por um cabo de fibra óptica ou a quantidade de armazenamento em um disco físico.		que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalm ente os parâmetro s AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentag e (Config Default: 80). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-1	Como você gerencia cotas de serviço e restrições? Para arquiteturas de workload baseadas em nuvem, existem cotas de serviço (que também são chamadas de limites de serviço). Essas cotas existem para evitar o provision amento acidental de mais recursos do que você precisa e para limitar as taxas de solicitaç ão nas operações de API, a fim de proteger os serviços contra uso abusivo. Também há restriçõe s de recursos, por exemplo, a taxa em que você pode propagar bits por um cabo de fibra óptica ou a quantidade de armazenamento em um disco físico.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-1	Como você gerencia cotas de serviço e restrições? Para arquiteturas de workload baseadas em nuvem, existem cotas de serviço (que também são chamadas de limites de serviço). Essas cotas existem para evitar o provision amento acidental de mais recursos do que você precisa e para limitar as taxas de solicitaç ão nas operações de API, a fim de proteger os serviços contra uso abusivo. Também há restrições de recursos, por exemplo, a taxa em que você pode propagar bits por um cabo de fibra óptica ou a quantidade de armazenamento em um disco físico.	ecs-task-definition-memory-hard-limit	Limitar a memória máxima disponíve l para contêineres do Amazon Elastic Container Service (ECS) garante que não haja abuso no uso do recurso em caso de acesso mal-intencionado aos contêineres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-2	Como você planeja sua topologia de rede? Geralmente, existem workloads em vários ambientes . Isso inclui vários ambientes de nuvem (acessíveis ao público e privados) e, possivelmente, a infraestrutura de datacenter existente . Os planos devem incluir considera ções de rede, como conectividade intra e entre sistemas, gerenciamento de endereços IP públicos, gerenciam ento de endereços IP privados e resolução de nomes de domínio.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-2	Como você planeja sua topologia de rede? Geralmente, existem workloads em vários ambientes . Isso inclui vários ambientes de nuvem (acessíveis ao público e privados) e, possivelmente, a infraestrutura de datacenter existente . Os planos devem incluir considera ções de rede, como conectividade intra e entre sistemas, gerenciamento de endereços IP públicos, gerenciam ento de endereços IP privados e resolução de nomes de domínio.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-2	Como você planeja sua topologia de rede? Geralmente, existem workloads em vários ambientes . Isso inclui vários ambientes de nuvem (acessíveis ao público e privados) e, possivelmente, a infraestrutura de datacenter existente . Os planos devem incluir considera ções de rede, como conectividade intra e entre sistemas, gerenciamento de endereços IP públicos, gerenciam ento de endereços IP privados e resolução de nomes de domínio.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-5	Como você projeta interações em um sistema distribuído para mitigar ou resistir a falhas? Os sistemas distribuídos dependem de redes de comunicação para interconectar componentes, como servidores ou serviços. A workload deve operar de forma confiável, apesar da perda de dados ou da latência nessas redes. Os componentes do sistema distribuído devem operar de uma maneira que não afete negativamente outros componentes ou a workload. Essas práticas recomendadas evitam falhas e melhoram o tempo médio entre falhas (MTBF).	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	beanstalk-enhanced -health-reporting- enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	ecs-container-insights-enabled	O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Elastic Container Service (ECS) e de suas AWS soluções. O Container Insights também fornece informações de diagnóstico, como falhas de reinicialização de contêiner, para ajudar a isolar problemas e resolvê-los rapidamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapass ados ou ocorrerem eventos significa tivos. O monitoram ento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automatic amente em resposta.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-6	Como você monitora os recursos da workload? Logs e métricas são ferramentas avançadas para obter informações sobre a integridade da workload. Você pode configurar a workload para monitorar logs e métricas e enviar notificações quando os limites forem ultrapassados ou ocorrerem eventos significativos. O monitoramento permite que a workload reconheça quando os limites de baixo desempenho são ultrapassados ou ocorrem falhas, para que ela possa se recuperar automaticamente em resposta.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-7	Como você projeta a workload para se adaptar às alterações na demanda? Uma workload escalável fornece elasticidade para adicionar ou remover recursos automaticamente, de modo que eles correspondam perfeitamente à demanda atual em determinado momento.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-7	Como você projeta a workload para se adaptar às alterações na demanda? Uma workload escalável fornece elasticidade para adicionar ou remover recursos automaticamente, de modo que eles correspondam perfeitamente à demanda atual em determinado momento.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-7	Como você projeta a workload para se adaptar às alterações na demanda? Uma workload escalável fornece elasticidade para adicionar ou remover recursos automaticamente, de modo que eles correspondam perfeitamente à demanda atual em determinado momento.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-8	Como você implementa a alteração? Alterações controladas são necessárias para implantar novas funcionalidades e garantir que as workloads e o ambiente operacional estejam executando software conhecido e possam ser corrigidas ou substituídas de maneira previsível. Se essas alterações não forem controladas, será difícil prever o efeito dessas alterações ou resolver os problemas que surgem por causa delas.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-8	Como você implementa a alteração? Alterações controladas são necessárias para implantar novas funcionalidades e garantir que as workloads e o ambiente operacional estejam executando software conhecido e possam ser corrigidas ou substituídas de maneira previsível. Se essas alterações não forem controladas, será difícil prever o efeito dessas alterações ou resolver os problemas que surgem por causa delas.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-8	Como você implementa a alteração? Alterações controladas são necessárias para implantar novas funcionalidades e garantir que as workloads e o ambiente operacional estejam executando software conhecido e possam ser corrigidas ou substituídas de maneira previsível. Se essas alterações não forem controladas, será difícil prever o efeito dessas alterações ou resolver os problemas que surgem por causa delas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-8	Como você implementa a alteração? Alterações controladas são necessárias para implantar novas funcionalidades e garantir que as workloads e o ambiente operacional estejam executando software conhecido e possam ser corrigidas ou substituídas de maneira previsível. Se essas alterações não forem controladas, será difícil prever o efeito dessas alterações ou resolver os problemas que surgem por causa delas.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicações e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-9	Como você faz backup dos dados? Faça backup de dados, aplicaçõe s e configurações para atender às suas necessidades de objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO).	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	clb-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibi lidade diferentes para garantir que sua função esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	opensearch-data-node-fault-tolerance	O Amazon OpenSearch Service (OpenSearch Service) exige pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um domínio OpenSearch de serviço com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
REL-10	Como você usa o isolamento de falhas para proteger a workload? Os limites isolados de falhas limitam o efeito de uma falha em uma workload a um número limitado de componentes. Os componentes fora do limite não são afetados pela falha. Ao usar vários limites isolados de falhas, é possível limitar o impacto na workload.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

Modelo

O modelo está disponível em GitHub: Operational Best Practices for AWS Well-Architected Reliability Pillar.

Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o pilar de segurança do Well-Architected Framework da Amazon Web Services e as regras de configuração gerenciadas. AWS Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais dos princípios de design do pilar. Uma categoria do Well-Architected Framework pode estar relacionada a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-	account-part-of-or ganizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configura ções da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os a todas as áreas. Manter-se atualizado com as recomendações do setor AWS e a inteligência de ameaças ajuda você a desenvolver seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomendadas abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacional em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizado com as recomendações do setor AWS e a inteligência de ameaças ajuda você a desenvolver seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomendadas abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacional em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizado com as recomendações do setor AWS e a inteligência de ameaças ajuda você a desenvolver seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomenda das abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacion al em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizad o com as recomenda ções do setor AWS e a inteligência de ameaças ajuda você a desenvolv er seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	ec2-managedinstanc e-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-1	Como você opera seu workload com segurança? Para operar seu workload com segurança, você deve aplicar as práticas recomendadas abrangentes em todas as áreas de segurança. Pegue os requisitos e processos que você definiu em excelência operacional em um nível organizacional e de workload e aplique-os a todas as áreas. Manter-se atualizado com as recomendações do setor AWS e a inteligência de ameaças ajuda você a desenvolver seu modelo de ameaças e seus objetivos de controle. A automação dos processos, testes e validação de segurança permite que você escale suas operações de segurança.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidad es da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidad es de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidades que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativos. São membros da sua organização ou usuários externos com quem você colabora e que interagem com	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidades que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativos. São membros da sua organização ou usuários externos com quem você colabora e que interagem com	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidades que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativos. São membros da sua organização ou usuários externos com quem você colabora e que interagem com	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidad es da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidad es de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. São membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	secretsmanager-rot ation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidades que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativos. Eles são membros da sua organização ou usuários externos com quem você colabora e que interagem com	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. Eles são membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	secretsmanager-sec ret-periodic-rotation	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação periódica ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido. O valor padrão é 90 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. Eles são membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	secretsmanager-sec ret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedFor Days (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. Eles são membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	secretsmanager-usi ng-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-2	Como você gerencia identidades de pessoas e de máquinas? Há dois tipos de identidad es que você precisa gerenciar ao abordar a operação de cargas de trabalho seguras AWS . Entender o tipo de identidade que você precisa gerenciar e conceder acesso ajuda a garantir que as identidades certas tenham acesso aos recursos certos nas condições certas. Identidades humanas: seus administradores, desenvolvedores, operadores e usuários finais precisam de uma identidade para acessar seus AWS ambientes e aplicativ os. Eles são membros da sua organizaç ão ou usuários externos com quem você colabora e que interagem com	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	seus AWS recursos por meio de um navegador da Web, aplicativo cliente ou ferramentas interativas de linha de comando. Identidades da máquina: seus aplicativos de serviço, ferramentas operacionais e cargas de trabalho exigem uma identidade para fazer solicitações aos AWS serviços, por exemplo, para ler dados. Essas identidades incluem máquinas em execução em seu AWS ambiente, como instâncias do Amazon EC2 ou funções AWS Lambda. Você também pode gerenciar identidades de máquina para partes externas que precisam de acesso. Além disso, você também pode ter máquinas fora dela AWS que precisem		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acessar seu AWS ambiente.		
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégi o mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ecs-containers-non privileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégi o mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	efs-access-point-e nforce-user-identity	Para ajudar na implementação do princípio de privilégi o mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configura da no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriados.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-user-group-membership-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantind o que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Cada componente ou recurso de seu workload precisa ser acessado por administradores, usuários finais ou outros componentes. Tenha uma definição clara de quem ou o que deve ter acesso a cada component e, escolha o tipo de identidade e o método de autenticação e autorização apropriad os.	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Estabeleça controles comuns que restrinja m o acesso a todas as identidades em sua organização. Por exemplo, você pode restringir o acesso a AWS regiões específicas ou impedir que seus operadore s excluam recursos comuns, como uma função do IAM usada pela sua equipe de segurança central.	account-part-of-or ganizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configura ções da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuamente as descobertas que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuamente as descobertas que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuamente as descobertas que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedFor Days (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuam ente as descobert as que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-3	Como você gerencia as permissões para pessoas e máquinas? Monitore continuamente as descobertas que destacam o acesso entre contas e público. Reduza o acesso público e o acesso entre contas somente aos recursos que exigem esse tipo de acesso.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-4	Como detectar e investigar eventos de segurança? Capture e analise eventos de logs e métricas para obter visibilidade. Tomar medidas em relação aos eventos de segurança e possíveis ameaças para ajudar a proteger seu workload.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, comprome er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	ec2-instance-multiple-eni-check	Essa regra verifica se suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) têm vários ENIs. Ter vários ENIs pode causar instâncias com hospedagem dupla, ou seja, instâncias com várias sub-redes . Isso pode aumentar a complexidade da segurança da rede e introduzir caminhos e acessos de rede não intencionais.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecion ar e controlar solicitaç ões da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-5	Como você protege seus recursos de rede? Qualquer workload que tenha alguma forma de conectividade de rede, seja a internet ou uma rede privada, requer várias camadas de defesa para ajudar a se proteger contra ameaças externas e internas baseadas na rede.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ecs-container-insights-enabled	O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Elastic Container Service (ECS) e de suas AWS soluções. O Container Insights também fornece informações de diagnóstico, como falhas de reinicialização de contêiner, para ajudar a isolar problemas e resolvê-los rapidamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrad o um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataform a. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataform a.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-instance-multiple-eni-check	Essa regra verifica se suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) têm vários ENIs. Ter vários ENIs pode causar instâncias com hospedagem dupla, ou seja, instâncias com várias sub-redes . Isso pode aumentar a complexidade da segurança da rede e introduzir caminhos e acessos de rede não intencionais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computaci onais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêiner es, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-6	Como você protege seus recursos computacionais? Os recursos computacionais em seu workload exigem várias camadas de defesa para ajudar na proteção contra ameaças externas e internas. Os recursos de computação incluem instâncias do EC2, contêineres, funções AWS Lambda, serviços de banco de dados, dispositivos de IoT e muito mais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implementando vários controles para reduzir o risco de acesso não autorizado ou manuseio incorreto.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenad os no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	kms-cmk-not-schedu led-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programad as para exclusão, caso alguma delas sido programada de maneira não intencion al.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	dynamodb-table-encrypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implementando vários controles para reduzir o risco de acesso não autorizado ou manuseio incorreto.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implementando vários controles para reduzir o risco de acesso não autorizado ou manuseio incorreto.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implementando vários controles para reduzir o risco de acesso não autorizado ou manuseio incorreto.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	account-part-of-or ganizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configura ções da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SEG-8	Como você protege seus dados em repouso? Proteja seus dados em repouso implement ando vários controles para reduzir o risco de acesso não autorizad o ou manuseio incorreto.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizad os.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizad os.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizados.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SEG-9	Como você protege seus dados em trânsito? Proteja seus dados em trânsito implementando vários controles para reduzir o risco de acesso ou perda não autorizad os.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

Modelo

O modelo está disponível em GitHub: Operational Best Practices for AWS Well-Architected Security Pillar.

Práticas recomendadas operacionais para BCP e DR

Esse pacote de conformidade contém AWS Config regras baseadas no BCP e no DR interno. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para BCP e DR.

Práticas recomendadas operacionais para o BNM RMit

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Risk Management in Technology (RMiT) do Bank Negara Malaysia (BNM) e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles BNM RMit. Um controle do CJIS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	deve tomar medidas apropriadas para garantir a existênci a de controles e processos robustos para gerenciar as chaves de criptogra fia. Quando isso envolver a confiança em avaliações de terceiros, a instituiç ão financeira deverá considerar se essa confiança é consisten te com a propensão e a tolerância ao risco da instituição financeir a. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessári os para apoiar os controles criptográ ficos e ao risco de redução da visibilid ade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.18	Uma instituição financeira deve realizar a devida diligência e avaliar os controles criptográficos associados à tecnologia utilizada, a fim de proteger a confidencialidade, integridade, autenticação, autorização e não repúdio das informações. Quando uma instituição financeira não gera suas próprias chaves de criptografia, ela deve tomar medidas apropriadas para garantir a existência de controles e processos robustos para gerenciar as chaves de criptografia. Quando isso envolver a confiança em avaliações de terceiros, a instituição financeira deverá considerar se essa confiança é consistente com a propensão e a tolerância ao risco	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	da instituição financeira. Uma instituição financeira também deve dar a devida atenção aos recursos do sistema necessários para apoiar os controles criptográficos e ao risco de redução da visibilidade do tráfego de rede dos dados que foram criptografados.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.20	Uma instituição financeira deve armazenar chaves criptográficas públicas em um certificado emitido por uma autoridade de certificação, conforme apropriado ao nível de risco. Esses certificados associados aos clientes serão emitidos por autoridades de certificação reconhecidas. A instituição financeira deve garantir que a implementação de protocolos de autenticação e assinatura utilizando tais certificados esteja sujeita a uma forte proteção para garantir que a utilização de chaves criptográficas privadas correspondentes aos certificados de utilizador seja juridicamente vinculativa e irrefutável. A emissão inicial e a subsequente	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	renovação de tais certificados devem ser consistentes com as práticas recomendadas do setor e com as especificações legais/regulamentares aplicáveis.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.20	Uma instituição financeira deve armazenar chaves criptográficas públicas em um certificado emitido por uma autoridade de certificação, conforme apropriado ao nível de risco. Esses certificados associados aos clientes serão emitidos por autoridades de certificação reconhecidas. A instituição financeira deve garantir que a implementação de protocolos de autenticação e assinatura utilizando tais certificados esteja sujeita a uma forte proteção para garantir que a utilização de chaves criptográficas privadas correspondentes aos certificados de utilizador seja juridicamente vinculativa e irrefutável. A emissão inicial e a subsequente	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	renovação de tais certificados devem ser consistentes com as práticas recomendadas do setor e com as especificações legais/regulamentares aplicáveis.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
10,27	Uma instituiç ão financeira deve estabelec er mecanismos de monitorização em tempo real para acompanha r a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionávei s aos administr adores.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,27	Uma instituição financeira deve estabelecer mecanismos de monitorização em tempo real para acompanhar a utilização da capacidade e o desempenho dos principais processos e serviços. Esses mecanismos de monitoramento deverão ser capazes de fornecer alertas oportunos e acionáveis aos administradores.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,34	Uma instituição financeira deve garantir que os serviços de rede dos seus sistemas críticos são confiávei s e não têm SPOF, a fim de proteger os sistemas críticos contra potenciai s falhas de rede e ameaças cibernéticas.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,34	Uma instituição financeira deve garantir que os serviços de rede dos seus sistemas críticos são confiávei s e não têm SPOF, a fim de proteger os sistemas críticos contra potenciai s falhas de rede e ameaças cibernéticas.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,35	Uma instituiç ão financeira deve estabelec er processos de monitoramento de largura de banda da rede em tempo real e métricas de resiliência de serviço de rede correspon dentes para sinalizar qualquer utilização excessiva de largura de banda e interrupç ões do sistema devido a congestionamento de largura de banda e falhas de rede. Isso inclui análise de tráfego para detectar tendências e anomalias.	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,35	Uma instituição financeira deve estabelecer processos de monitoramento de largura de banda da rede em tempo real e métricas de resiliência de serviço de rede correspondentes para sinalizar qualquer utilização excessiva de largura de banda e interrupções do sistema devido a congestionamento de largura de banda e falhas de rede. Isso inclui análise de tráfego para detectar tendências e anomalias.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,35	Uma instituição financeira deve estabelecer processos de monitoramento de largura de banda da rede em tempo real e métricas de resiliência de serviço de rede correspondentes para sinalizar qualquer utilização excessiva de largura de banda e interrupções do sistema devido a congestionamento de largura de banda e falhas de rede. Isso inclui análise de tráfego para detectar tendências e anomalias.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,35	Uma instituição financeira deve estabelecer processos de monitoramento de largura de banda da rede em tempo real e métricas de resiliência de serviço de rede correspondentes para sinalizar qualquer utilização excessiva de largura de banda e interrupções do sistema devido a congestionamento de largura de banda e falhas de rede. Isso inclui análise de tráfego para detectar tendências e anomalias.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,36	Uma instituição financeira deve garantir que os serviços de rede que suportam sistemas críticos sejam projetados e implementados para garantir a confidencialidade, integridade e disponibilidade dos dados.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10,36	Uma instituição financeira deve garantir que os serviços de rede que suportam sistemas críticos sejam projetados e implementados para garantir a confidencialidade, integridade e disponibilidade dos dados.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,36	Uma instituição financeira deve garantir que os serviços de rede que suportam sistemas críticos sejam projetados e implementados para garantir a confidencialidade, integridade e disponibilidade dos dados.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
10,36	Uma instituição financeira deve garantir que os serviços de rede que suportam sistemas críticos sejam projetados e implementados para garantir a confidencialidade, integridade e disponibilidade dos dados.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,36	Uma instituição financeira deve garantir que os serviços de rede que suportam sistemas críticos sejam projetados e implementados para garantir a confidenc ialidade, integridade e disponibilidade dos dados.	nlb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para seus Network Load Balancers (NLBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,38	Uma instituição financeira deve garantir que registros de dispositivos de rede suficientes e relevantes sejam retidos para investigações e fins forenses por pelo menos três anos.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudar você a restringir permissões e autorizações de acesso, garantindo que os usuários do IAM sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	sagemaker-notebook -no-direct-internet- access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapartes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutenção da propriedade, o controle e o gerenciamento de todos os dados relativos às informações dos clientes e das contrapartes, dos dados proprietários e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,51	Uma instituição financeira deve implementar proteções apropriadas nas informações de clientes e contrapar tes e nos dados proprietários ao usar serviços em nuvem para proteger contra divulgação e acesso não autorizados. Isso inclui a manutençã o da proprieda de, o controle e o gerenciamento de todos os dados relativos às informaçõ es dos clientes e das contrapartes, dos dados proprietá rios e dos serviços hospedados na nuvem, incluindo o gerenciamento das chaves criptográficas relevantes.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	account-part-of-or ganizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configura ções da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-policy-no-stat ements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-user-group-mem bership-check	AWS O Identity and Access Managemen t (IAM) pode ajudar você a restringi r permissões e autorizações de acesso, garantindo que os usuários do IAM sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos.	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,52	Uma instituição financeira deve implementar uma política de controle de acesso adequada para a identific ação, autenticação e autorização de usuários (usuários internos e externos, tais como prestadores de serviços terceiros). Isso deve abordar controles de acesso à tecnologia lógica e física que sejam proporcionais ao nível de risco de acesso não autorizad o aos seus sistemas tecnológicos	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)(h)(i)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s em sua política de controle de acesso: (b) empregue direitos de acesso de “privilégio mínimo” ou com base na “necessidade”, em que somente as permissões mínimas suficientes sejam concedidas a usuários legítimos para exercer suas funções; (h) limite e controle o compartilhamento de ID de usuário e senhas entre vários usuários; e (i) controle o uso de convenções genéricas de nomenclatura de ID de usuário em favor de pessoas com IDs pessoais mais identificáveis.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilég io mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilég io mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilég io mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilég io mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeira deve considerar os seguintes princípios na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilégio mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeira deve considerar os seguintes princípios na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilégio mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudar você a restringir permissões e autorizações de acesso, garantindo que os usuários do IAM sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(b)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controlo de acesso: (b) empregue direitos de acesso de "privilég io mínimo" ou na base da "necessidade de ter", em que somente as permissões mínimas suficientes são concedidas aos usuários legítimos para desempenharem as suas funções;	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(c)(f)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controle de acesso: (c) empregue direitos de acesso limitados no tempo que restrinja m o acesso a um período específico, incluindo direitos de acesso concedido s a prestadores de serviços; (f) adote uma autenticação mais forte para atividades críticas, inclusive para acesso remoto	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(f)(h)	Ao observar o parágrafo 10.52, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controle de acesso: (f) adote uma autentica ção mais forte para atividades críticas, inclusive para acesso remoto; (h) limite e controle o compartil hamento de ID de usuário e senhas entre vários usuários	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(f)(h)	Ao observar o parágrafo 10.54, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controle de acesso: (f) adote uma autentica ção mais forte para atividades críticas, inclusive para acesso remoto; (h) limite e controle o compartil hamento de ID de usuário e senhas entre vários usuários	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.53(f)(h)	Ao observar o parágrafo 10.54, uma instituição financeir a deve considerar os seguintes princípio s na sua política de controle de acesso: (f) adote uma autentica ção mais forte para atividades críticas, inclusive para acesso remoto; (h) limite e controle o compartil hamento de ID de usuário e senhas entre vários usuários	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.54	Uma instituição financeira deve empregar processos de autenticação robustos para garantir a autenticidade das identidades em uso. Os mecanismos de autenticação devem ser proporcionais à criticidade das funções e adotar pelo menos um ou mais desses três fatores básicos de autenticação, a saber, algo que o usuário sabe (por exemplo, senha, PIN), algo que o usuário possui (por exemplo, cartão inteligente, dispositivo de segurança) e algo que o usuário é (por exemplo, caracterí sticas biométricas, como impressão digital ou padrão retinal).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.54	Uma instituição financeira deve empregar processos de autenticação robustos para garantir a autenticidade das identidades em uso. Os mecanismos de autenticação devem ser proporcionais à criticidade das funções e adotar pelo menos um ou mais desses três fatores básicos de autenticação, a saber, algo que o usuário sabe (por exemplo, senha, PIN), algo que o usuário possui (por exemplo, cartão inteligente, dispositivo de segurança) e algo que o usuário é (por exemplo, caracterí sticas biométricas, como impressão digital ou padrão retinal).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.54	Uma instituição financeira deve empregar processos de autenticação robustos para garantir a autenticidade das identidades em uso. Os mecanismos de autenticação devem ser proporcionais à criticidade das funções e adotar pelo menos um ou mais desses três fatores básicos de autenticação, a saber, algo que o usuário sabe (por exemplo, senha, PIN), algo que o usuário possui (por exemplo, cartão inteligente, dispositivo de segurança) e algo que o usuário é (por exemplo, caracterí sticas biométricas, como impressão digital ou padrão retinal).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,55	Uma instituição financeira deve rever e adaptar periodica mente as suas práticas de utilizaçã o de senhas para aumentar a resiliência contra a evolução dos ataques. Isso inclui a geração eficaz e segura de senhas. Deve haver controles apropriados para verificar a força das senhas criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,56	Os métodos de autenticação que dependem de mais de um fator normalmen te são mais difíceis de comprometer do que um sistema de fator único. Com isso em mente, as instituições financeir as são incentivadas a projetar e implement ar adequadamente (especialmente em sistemas de alto risco ou de “logon único”) autenticação multifato r (MFA) que seja mais confiável e forneça dissuasores de fraude mais fortes	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,56	Os métodos de autenticação que dependem de mais de um fator normalmente são mais difíceis de comprometer do que um sistema de fator único. Com isso em mente, as instituições financeiras são incentivadas a projetar e implementar adequadamente (especialmente em sistemas de alto risco ou de “logon único”) autenticação multifator (MFA) que seja mais confiável e forneça dissuasores de fraude mais fortes	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,56	Os métodos de autenticação que dependem de mais de um fator normalmente são mais difíceis de comprometer do que um sistema de fator único. Com isso em mente, as instituições financeiras são incentivadas a projetar e implementar adequadamente (especialmente em sistemas de alto risco ou de “logon único”) autenticação multifator (MFA) que seja mais confiável e forneça dissuasores de fraude mais fortes	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudar você a restringir permissões e autorizações de acesso, garantindo que os usuários do IAM sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivame nte gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registrad as para auditoria e investigações. Os registros de atividade s devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,59	Uma instituição financeira deve garantir que (a) os controles de acesso aos sistemas de toda a empresa sejam efetivamente gerenciados e monitorados; e (b) as atividades dos usuários em sistemas críticos são registradas para auditoria e investigações. Os registros de atividades devem ser mantidos por pelo menos três anos e revisados regularmente em tempo hábil.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,60	Ao cumprir o requisito do parágrafo 10.59, as grandes instituiç ões financeiras são obrigadas a (a) implementar um sistema de gerenciam ento de acesso de identidade para gerenciar e monitorar eficazmente o acesso dos usuários aos sistemas de toda a empresa; e (b) implantar ferramentas de auditoria automatiz adas para sinalizar quaisquer anomalias.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,60	Ao cumprir o requisito do parágrafo 10.61, as grandes instituiç ões financeiras são obrigadas a (a) implementar um sistema de gerenciam ento de acesso de identidade para gerenciar e monitorar eficazmente o acesso dos usuários aos sistemas de toda a empresa; e (b) implantar ferramentas de auditoria automatiz adas para sinalizar quaisquer anomalias.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,60	Ao cumprir o requisito do parágrafo 10.61, as grandes instituiç ões financeiras são obrigadas a (a) implementar um sistema de gerenciam ento de acesso de identidade para gerenciar e monitorar eficazmente o acesso dos usuários aos sistemas de toda a empresa; e (b) implantar ferramentas de auditoria automatiz adas para sinalizar quaisquer anomalias.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,61	Uma instituição financeira deve garantir que sistemas críticos não sejam executados em sistemas desatualizados com vulnerabilidades de segurança conhecidas ou sistemas de tecnologia end-of-life (EOL). Nesse sentido, uma instituição financeira deve atribuir claramente responsabilidades às funções identificadas: (a) monitorar continuamente e implementar os lançamentos de patches mais recentes em tempo hábil; e (b) identificar sistemas tecnológicos críticos que estão se aproximando do fim da vida útil para obter mais medidas corretivas.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,61	Uma instituição financeira deve garantir que sistemas críticos não sejam executados em sistemas desatualizados com vulnerabilidades de segurança conhecidas ou sistemas de tecnologia end-of-life (EOL). Nesse sentido, uma instituição financeira deve atribuir claramente responsabilidades às funções identificadas: (a) monitorar continuamente e implementar os lançamentos de patches mais recentes em tempo hábil; e (b) identificar sistemas tecnológicos críticos que estão se aproximando do fim da vida útil para obter mais medidas corretivas.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,61	Uma instituição financeira deve garantir que sistemas críticos não sejam executados em sistemas desatualizados com vulnerabilidades de segurança conhecidas ou sistemas de tecnologia end-of-life (EOL). Nesse sentido, uma instituição financeira deve atribuir claramente responsabilidades às funções identificadas: (a) monitorar continuamente e implementar os lançamentos de patches mais recentes em tempo hábil; e (b) identificar sistemas tecnológicos críticos que estão se aproximando do fim da vida útil para obter mais medidas corretivas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,61	Uma instituição financeira deve garantir que sistemas críticos não sejam executados em sistemas desatualizados com vulnerabilidades de segurança conhecidas ou sistemas de tecnologia end-of-life (EOL). Nesse sentido, uma instituição financeira deve atribuir claramente responsabilidades às funções identificadas: (a) monitorar continuamente e implementar os lançamentos de patches mais recentes em tempo hábil; e (b) identificar sistemas tecnológicos críticos que estão se aproximando do fim da vida útil para obter mais medidas corretivas.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10,61	Uma instituição financeira deve garantir que sistemas críticos não sejam executados em sistemas desatualizados com vulnerabilidades de segurança conhecidas ou sistemas de tecnologia end-of-life (EOL). Nesse sentido, uma instituição financeira deve atribuir claramente responsabilidades às funções identificadas: (a) monitorar continuamente e implementar os lançamentos de patches mais recentes em tempo hábil; e (b) identificar sistemas tecnológicos críticos que estão se aproximando do fim da vida útil para obter mais medidas corretivas.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(a)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (a) confidencialidade e integridade das informações e transações de clientes e contrapartes	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	nlb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para seus NetworkLoad balanceadores (NLBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(b)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (b) confiabilidade dos serviços prestados por meio de canais e dispositivos com interrupção mínima dos serviços	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológi ca no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(d)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (d) trilha de auditoria suficiente e monitoramento de transações anômalas	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.64(e)	Uma instituição financeira deve implementar controles robustos de segurança tecnológica no fornecimento de serviços digitais que garantam o seguinte: (e) capacidade de identificar e reverter ao ponto de recuperação antes do incidente ou interrupção do serviço	s3-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus buckets do Amazon Simple Storage Service (S3) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.7	Uma instituiç ão financeira deve implement ar ferramentas eficazes para apoiar a monitoriz ação contínua e proativa e a deteção oportuna de atividade s anômalas na sua infraestrutura tecnológica. O escopo de monitoramento deve abranger todos os sistemas críticos, incluindo a infraestr utura de suporte.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.7	Uma instituiç ão financeira deve implement ar ferramentas eficazes para apoiar a monitoriz ação contínua e proativa e a deteção oportuna de atividade s anômalas na sua infraestrutura tecnológica. O escopo de monitoramento deve abranger todos os sistemas críticos, incluindo a infraestr utura de suporte.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.8	Uma instituição financeira deve garantir que as suas operações de cibersegurança previnem e detectam continuamente qualquer potencial comprometimento dos seus controles de segurança ou enfraquecimento da sua postura de segurança. Para as grandes instituições financeiras, isso deve incluir a realização de uma avaliação trimestral da vulnerabilidade dos componentes da rede externa e interna que são compatíveis com todos os sistemas críticos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.8	Uma instituição financeira deve garantir que as suas operações de cibersegurança previnem e detectam continuamente qualquer potencial comprometimento dos seus controles de segurança ou enfraquecimento da sua postura de segurança. Para as grandes instituições financeiras, isso deve incluir a realização de uma avaliação trimestral da vulnerabilidade dos componentes da rede externa e interna que são compatíveis com todos os sistemas críticos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.18(c)(f)	O SOC deve ser capaz de desempenhar as seguintes funções: (c) gerenciamento de vulnerabilidades; (f) fornecimento de reconhecimento situacional para detectar adversários e ameaças, incluindo análises e operações de inteligência sobre ameaças, e monitorar indicadores de comprometimento (IOC). Isso inclui análise comportamental avançada para detectar malware sem assinatura e sem arquivo e para identificar anomalias que possam representar ameaças à segurança, inclusive em endpoints e camadas de rede.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.18(c)(f)	O SOC deve ser capaz de desempenhar as seguintes funções: (c) gerenciamento de vulnerabilidades; (f) fornecimento de reconhecimento situacional para detectar adversários e ameaças, incluindo análises e operações de inteligência sobre ameaças, e monitorar indicadores de comprometimento (IOC). Isso inclui análise comportamental avançada para detectar malware sem assinatura e sem arquivo e para identificar anomalias que possam representar ameaças à segurança, inclusive em endpoints e camadas de rede.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.18(c)(f)	O SOC deve ser capaz de desempenhar as seguintes funções: (c) gerenciamento de vulnerabilidades; (f) fornecimento de reconhecimento situacional para detectar adversários e ameaças, incluindo análises e operações de inteligência sobre ameaças, e monitorar indicadores de comprometimento (IOC). Isso inclui análise comportamental avançada para detectar malware sem assinatura e sem arquivo e para identificar anomalias que possam representar ameaças à segurança, inclusive em endpoints e camadas de rede.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.1	Realize revisões periódicas nas configurações e regras de todos os dispositivos de segurança. Use ferramentas automatizadas para revisar e monitorar alterações nas configurações e nas definições de regras.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.1	Realize revisões periódicas nas configurações e regras de todos os dispositivos de segurança. Use ferramentas automatizadas para revisar e monitorar alterações nas configurações e nas definições de regras.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Apêndice 5.5(b)	Certifique-se de que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (b) uso de túneis seguros, como Transport Layer Security (TLS) e IPsec de Rede Privada Virtual (VPN)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(c)	Garanta que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (c) implantar servidores de teste com defesas e proteção perimetra is adequadas, como firewall, IPS e antivírus.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(c)	Garanta que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (c) implantar servidores de teste com defesas e proteção perimetra is adequadas, como firewall, IPS e antivírus.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.5(c)	Garanta que os controles de segurança para conexões de rede server-to-server externas incluam o seguinte: (c) implantar servidores de teste com defesas e proteção perimetra is adequadas, como firewall, IPS e antivírus.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 5.6	Garanta que os controles de segurança para acesso remoto ao servidor incluam o seguinte: (a) restringir o acesso apenas a dispositivos de endpoint protegidos e bloqueados; (b) usar túneis seguros como TLS e VPN IPSec; (c) implantar servidor “gateway” com defesas e proteção de perímetro adequadas, como firewall, IPS e antivírus; e (d) fechar os portos relevantes imediatamente após a expiração do acesso remoto.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (a)	Uma instituição financeira deve conceber uma arquitetura de nuvem robusta e garantir que tal conceção esteja de acordo com as normas internacionais relevantes para a aplicação pretendida.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (b)	Uma instituição financeira é incentiva da a adotar princípio s de confiança zero para fornecer uma arquitetura cibernética resilient e, adotando uma mentalidade de “supor violação”, abrangendo microssegmentação, direitos de acesso de “negação defense-i n-depth por padrão” e “privilégio mínimo” e conduzindo uma inspeção profunda e validação contínua, quando aplicável.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (b)	Uma instituição financeira é incentiva da a adotar princípio s de confiança zero para fornecer uma arquitetura cibernética resilient e, adotando uma mentalidade de “supor violação”, abrangendo microssegmentação, direitos de acesso de “negação defense-i n-depth por padrão” e “privilégio mínimo” e conduzindo uma inspeção profunda e validação contínua, quando aplicável.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (b)	Uma instituição financeira é incentiva da a adotar princípio s de confiança zero para fornecer uma arquitetura cibernética resilient e, adotando uma mentalidade de “supor violação”, abrangendo microssegmentação, direitos de acesso de “negação defense-i n-depth por padrão” e “privilégio mínimo” e conduzindo uma inspeção profunda e validação contínua, quando aplicável.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (b)	Uma instituição financeira é incentiva da a adotar princípio s de confiança zero para fornecer uma arquitetura cibernética resilient e, adotando uma mentalidade de “supor violação”, abrangendo microssegmentação, direitos de acesso de “negação defense-i n-depth por padrão” e “privilégio mínimo” e conduzindo uma inspeção profunda e validação contínua, quando aplicável.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (c)	Uma instituição financeira deve usar a mais recente abordagem de arquitetura de rede e conceitos e soluções de design de rede apropriados para gerenciar e monitorar a segurança granular da rede e o fornecimento centralizado de rede no gerenciamento da complexidade do ambiente de rede em nuvem.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (c)	Uma instituição financeira deve usar a mais recente abordagem de arquitetura de rede e conceitos e soluções de design de rede apropriados para gerenciar e monitorar a segurança granular da rede e o fornecimento centralizado de rede no gerenciamento da complexidade do ambiente de rede em nuvem.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Apêndice 10 Parte B - 1 (d)	Uma instituição financeira deve estabelecer e utilizar canais de comunicação seguros e criptografados para migrar servidores físicos, aplicações ou dados para plataformas em nuvem.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (d)	Uma instituição financeira deve estabelecer e utilizar canais de comunicação seguros e criptografados para migrar servidores físicos, aplicações ou dados para plataformas em nuvem.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (f) i)	A utilização crescente de interfaces de programação de aplicações (API) pelas instituições financeiras para interconexão com fornecedores externos de serviços de aplicações poderia alcançar eficiência na prestação de novos serviços. No entanto, isso pode aumentar a superfície de ataques cibernéticos e qualquer má gestão pode amplificar o impacto de um incidente de segurança da informação. Uma instituição financeira deve garantir que as suas APIs estão sujeitas a mecanismos rigorosos de gestão e controle, que incluem o seguinte: i) as APIs devem ser concebidas para resiliência de serviço, a fim de evitar o risco de pontos únicos de	[api-gwv2-authorization-type-configured](#)	Garanta que sua rota de API v2 do Amazon API Gateway tenha um tipo de autorização definido para evitar acesso não autorizado aos recursos de back-end subjacentes.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	falha e configuradas de forma segura com controles de acesso apropriados;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (f) ii)	A utilização crescente de interfaces de programação de aplicações (API) pelas instituições financeir as para interconexão com fornecedores externos de serviços de aplicações poderia alcançar eficiênci a na prestação de novos serviços. No entanto, isso pode aumentar a superfíci e de ataques cibernéti cos e qualquer má gestão pode amplificar o impacto de um incidente de segurança da informação. Uma instituição financeir a deve garantir que as suas APIs estejam sujeitas a mecanismo s rigorosos de gerenciamento e controle, que incluem o seguinte: ii) as APIs devem ser rastreadas e monitoradas contra ataques cibernéti cos com medidas	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	adequadas de resposta a incidentes e ser desativadas em tempo hábil quando não estiverem mais em usar.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 1 (f) ii)	A utilização crescente de interfaces de programação de aplicações (API) pelas instituições financeir as para interconexão com fornecedores externos de serviços de aplicações poderia alcançar eficiênci a na prestação de novos serviços. No entanto, isso pode aumentar a superfíci e de ataques cibernéti cos e qualquer má gestão pode amplificar o impacto de um incidente de segurança da informação. Uma instituição financeir a deve garantir que as suas APIs estejam sujeitas a mecanismo s rigorosos de gerenciamento e controle, que incluem o seguinte: ii) as APIs devem ser rastreadas e monitoradas contra ataques cibernéti cos com medidas	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	adequadas de resposta a incidentes e ser desativadas em tempo hábil quando não estiverem mais em usar.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 2 (b) ii)	Uma instituição financeira deve aproveitar continuamente capacidades aprimoradas de nuvem para melhorar a segurança dos serviços em nuvem e as instituições financeiras são, entre outras coisas, incentivadas a: ii) usar práticas de infraestrutura imutáveis para implantação de serviços para reduzir o risco de falha, criando um ambiente com a versão estável mais recente do software. O monitoramento contínuo do ambiente de nuvem deve incluir a automatização da detecção de alterações em infraestruturas imutáveis para melhorar a revisão da conformidade e combater a evolução dos ataques cibernéticos	cloudformation-stack-notification-check	Para detectar alterações não intencionais nos AWS recursos subjacentes, certifique-se de que sua CloudFormation pilha esteja configurada para enviar notificações de eventos para um tópico do Amazon SNS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 3 (b) vi)	Uma instituição financeira deve garantir que as imagens de máquinas virtuais e de contêiner es sejam configura das, reforçada s e monitoradas adequadamente. Isso inclui o seguinte: vi) as imagens armazenadas estão sujeitas a monitoram ento de segurança contra acessos e alterações não autorizados.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituiç ões financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	aurora-resources-p rotected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituiç ões financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituições financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituições financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituições financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (a) i)	Como parte de uma capacidade de recuperação eficaz, as instituições financeiras devem garantir que os procedimentos existentes de backup e recuperação sejam alargados para cobrir os serviços em nuvem, o que inclui o seguinte: i) definir e formalizar a estratégia de backup e recuperação na fase de planeamento da adoção da nuvem;	s3-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus buckets do Amazon Simple Storage Service (S3) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (b)	Uma instituição financeira deve garantir que os procedimentos de backup e restauraç ão sejam testados periodicamente para validar as capacidad es de recuperaç ão. A frequência dos procedimentos de backup deve ser proporcional à criticidade do sistema e ao objetivo de ponto de recuperaç ão (RPO) do sistema. Ações corretivas devem ser tomadas imediatamente pela instituição financeir a para backups malsucedidos.	backup-plan-min-fr equency-and-min-re tention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyV alue parâmetros (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (c) i)	Uma instituição financeira deve garantir backup e recuperação suficientes da máquina virtual e do contêiner, incluindo definições de configuração de backup (para IaaS e PaaS, quando relevante), o que inclui o seguinte: i) garantir a capacidade de restaurar uma máquina virtual e um contêiner point-in-time conforme especificado pelos objetivos de recuperação do negócio;	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	autoscaling-multiple-az	Para garantir alta disponibilidade, certifique-se de que seu grupo do Auto Scaling esteja configurado para abranger várias zonas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibi lidade diferentes para garantir que sua função esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	nlb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para seus NetworkLo ad balanceadores (NLBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	rds-cluster-multi-az-enabled	Os clusters do Amazon Relationa l Database Service (Amazon RDS) devem ter a replicaçã o multi-AZ habilitad a para auxiliar na disponibilidade dos dados armazenad os. Cada zona de disponibilidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 5 (d) i)	Uma instituição financeira deve avaliar os requisito s de resiliência dos serviços em nuvem e identificar medidas adequadas que sejam proporcio nais à criticidade do sistema, para garantir a disponibi lidade do serviço em cenários adversos extremos. As instituiç ões financeiras devem considera r uma abordagem baseada no risco e adoptar progressi vamente controles de mitigação adequados para garantir a disponibilidade do serviço e mitigar o risco de concentra ção. Entre as opções viáveis estão: i) aproveitar os recursos de alta disponibilidade e redundância dos serviços em nuvem para garantir que os data centers de	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	produção tenham capacidade redundant e em diferentes zonas de disponibilidade;		failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidenc ialidade e integridade dos dados sensíveis armazenados na nuvem.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidenc ialidade e integridade dos dados sensíveis armazenados na nuvem.	backup-recovery-po int-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	eks-secrets-encrypted	Para ajudar a proteger os dados em repouso, certifique-se de que os clusters do Amazon Elastic Kubernetes Service (EKS) estejam configurados para ter os segredos do Kubernetes criptografados. Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (a)	Uma instituição financeira deve implementar técnicas de criptografia apropriadas e relevantes para proteger a confidencialidade e integridade dos dados sensíveis armazenados na nuvem.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (d)	À medida que aumenta o uso da adoção da nuvem, o gerenciamento de muitas chaves de criptografia usadas para proteger dados tornou-se mais complexo e pode apresentar novos desafios para as instituições financeir as. Uma instituição financeira deve adotar uma abordagem abrangente e centraliz ada ao gerenciamento de chaves, incluindo a utilização de um sistema centralizado de gerenciamento de chaves que possa lidar com gerações, armazenamento e distribuição de chaves de uma forma segura e escalável.	cmk-backing-key-ro tation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 8 (d)	À medida que aumenta o uso da adoção da nuvem, o gerenciamento de muitas chaves de criptografia usadas para proteger dados tornou-se mais complexo e pode apresentar novos desafios para as instituições financeir as. Uma instituição financeira deve adotar uma abordagem abrangente e centraliz ada ao gerenciamento de chaves, incluindo a utilização de um sistema centralizado de gerenciamento de chaves que possa lidar com gerações, armazenamento e distribuição de chaves de uma forma segura e escalável.	kms-cmk-not-schedu led-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programad as para exclusão, caso alguma delas sido programada de maneira não intencion al.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) ii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as instituições financeiras devem garantir o uso de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: ii) implementar "privilégios mínimos" e uma forte autenticação multifatorial (MFA), por exemplo, senha forte, token virtual, ferramenta de gerenciamento de	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acesso privilegiado e funções de verificador de criadores;		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) ii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as instituições financeiras devem garantir o uso de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: ii) implementar “privilégios mínimos” e uma forte autenticação multifatorial (MFA), por exemplo, senha forte, token virtual, ferramenta de gerenciamento de	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Esta regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo MFA para usuários do IAM.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acesso privilegiado e funções de verificador de criadores;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) ii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as instituições financeiras devem garantir o uso de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: ii) implementar “privilégios mínimos” e uma forte autenticação multifatorial (MFA), por exemplo, senha forte, token virtual, ferramenta de gerenciamento de	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acesso privilegiado e funções de verificador de criadores;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) ii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as instituições financeiras devem garantir o uso de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: ii) implementar "privilégios mínimos" e uma forte autenticação multifatorial (MFA), por exemplo, senha forte, token virtual, ferramenta de gerenciamento de	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	acesso privilegiado e funções de verificador de criadores;		
Apêndice 10 Parte B - 9 (a) iii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Com isso em vista, as instituições financeiras devem garantir a utilização de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: iii) empregar atribuição granular de direitos para usuários privilegiados;	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) iii)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Com isso em vista, as instituições financeiras devem garantir a utilização de controles fortes para acessar o plano de gerenciamento, que podem incluir o seguinte: iii) empregar atribuição granular de direitos para usuários privilegiados;	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) iv)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as Instituições financeiras devem assegurar a utilização de controles robustos de acesso ao plano de gerenciamento que podem incluir: iv) realizar monitoramento contínuo das atividades realizadas por usuários privilegiados;	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 9 (a) iv)	O plano de gerenciamento é uma diferença fundamental de segurança entre a infraestrutura tradicional e a computação em nuvem, onde o acesso remoto é compatível por padrão. Essa camada de acesso pode estar sujeita a ataques cibernéticos, comprometendo assim a integridade de toda a implantação da nuvem. Em vista disso, as Instituições financeiras devem assegurar a utilização de controles robustos de acesso ao plano de gerenciamento que podem incluir: iv) realizar monitoramento contínuo das atividades realizadas por usuários privilegiados;	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 12 (a)	Uma instituição financeira deve proteger os dados hospedados em serviços em nuvem, conforme exigido na seção Prevenção contra perda de dados (parágraf os 11.14 a 11.16) deste documento de política, incluindo a expansão da pegada de endpoint se a instituição financeir a permitir que seus funcionários usem seus próprios dispositi vos para acessar os dados confidenciais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 12 (a)	Uma instituição financeira deve proteger os dados hospedados em serviços em nuvem, conforme exigido na seção Prevenção contra perda de dados (parágraf os 11.14 a 11.16) deste documento de política, incluindo a expansão da pegada de endpoint se a instituição financeir a permitir que seus funcionários usem seus próprios dispositi vos para acessar os dados confidenciais.	macie-status-check	O Amazon Macie é um serviço de segurança de dados que usa machine learning (ML) e correspon dência de padrões para descobrir e ajudar a proteger dados confidenciais armazenados em buckets do Amazon Simple Storage Service (S3).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 14 (c) i)	Uma instituição financeira deve considerar as seguintes medidas adicionais no desenvolvimento de seu CIRP: i) aprimorar sua capacidade de detectar incidente s de violação de segurança para obter um gerenciam ento eficaz de incidentes, incluindo a capacidade de detectar vazamento de dados na dark web;	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Apêndice 10 Parte B - 14 (c) i)	Uma instituição financeira deve considerar as seguintes medidas adicionais no desenvolvimento de seu CIRP: i) aprimorar sua capacidade de detectar incidente s de violação de segurança para obter um gerenciam ento eficaz de incidentes, incluindo a capacidade de detectar vazamento de dados na dark web;	guardduty-non-arch ived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classific ando as descobert as por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégi as e prioridades de correção. Essa regra permite que você defina opcionalm ente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o BNM RMit.

Práticas recomendadas operacionais para o perfil de controle de nuvem médio do Canadian Centre for Cyber Security (CCCS)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Perfil de Controle de Nuvem Média do Centro Canadense de Segurança Cibernética (CCCS) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do CCCS Medium Cloud Control Profile. Um controle de perfil médio do Cloud Profile do CCCS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			capturados são vistos no Conteúdo do AWS CloudTrail Registro.
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(1)	Gerenciamento de contas do AC-2(1) | Gerenciamento automatizado de contas do sistema	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(3)	Gerenciamento de contas do AC-2(3) | Desativação de contas inativas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(3)	Gerenciamento de contas do AC-2(3) | Desativação de contas inativas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2(4)	Gerenciamento de contas do AC-2(4) | Ações de auditoria automatizadas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.A	Gerenciamento de contas do AC-2.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.B	Gerenciamento de contas do AC-2.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.C	Gerenciamento de contas do AC-2.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.D	Gerenciamento de contas do AC-2.D	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.E	Gerenciamento de contas do AC-2.E	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.F	Gerenciamento de contas do AC-2.F	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.G	Gerenciamento de contas do AC-2.G	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.H	Gerenciamento de contas do AC-2.H	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.l	Gerenciamento de contas do AC-2.l	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.I	Gerenciamento de contas do AC-2.I	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.J	Gerenciamento de contas do AC-2.J	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-2.K	Gerenciamento de contas do AC-2.K	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-3.A	Fiscalização de acesso do AC-3.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4(21)	Fiscalização de fluxo de informações do AC-4(21) | Separação física ou lógica dos fluxos de informações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-4.A	Fiscalização de fluxo de informações do AC-4.A	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-5.A	Separação de deveres do AC-5.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-5.A	Separação de deveres do AC-5.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-5.A	Separação de deveres do AC-5.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-5.A	Separação de deveres do AC-5.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-5.A	Separação de deveres do AC-5.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(1)	Privilégio mínimo do AC-6(1) | Autorização do acesso às funções de segurança	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(1)	Privilégio mínimo do AC-6(1) | Autorização do acesso às funções de segurança	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(1)	Privilégio mínimo do AC-6(1) | Autorização do acesso às funções de segurança	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(1)	Privilégio mínimo do AC-6(1) | Autorização do acesso às funções de segurança	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(1)	Privilégio mínimo do AC-6(1) | Autorização do acesso às funções de segurança	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(2)	Privilégio mínimo do AC-6(2) | Acesso não privilegiado para funções não relacionadas à segurança	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(2)	Privilégio mínimo do AC-6(2) | Acesso não privilegiado para funções não relacionadas à segurança	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(2)	Privilégio mínimo do AC-6(2) | Acesso não privilegiado para funções não relacionadas à segurança	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(2)	Privilégio mínimo do AC-6(2) | Acesso não privilegiado para funções não relacionadas à segurança	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(2)	Privilégio mínimo do AC-6(2) | Acesso não privilegiado para funções não relacionadas à segurança	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(5)	Privilégio mínimo do AC-6(5) | Contas privilegiadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(5)	Privilégio mínimo do AC-6(5) | Contas privilegiadas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(5)	Privilégio mínimo do AC-6(5) | Contas privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(5)	Privilégio mínimo do AC-6(5) | Contas privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6(9)	Privilégio mínimo do AC-6(9) | Auditoria do uso de funções privilegiadas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-AC-6(10)	Privilégio mínimo do AC-6(10) | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-AC-6(10)	Privilégio mínimo do AC-6(10) | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-AC-6(10)	Privilégio mínimo do AC-6(10) | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-AC-6(10)	Privilégio mínimo do AC-6(10) | Proibição de usuários não privilegiados de executar funções privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-AC-6(10)	Privilégio mínimo do AC-6(10) | Proibição de usuários não privilegiados de executar funções privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-6.A	Privilégio mínimo do AC-6.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(1)	Acesso remoto do AC-17(1) | Monitoramento e controle automatizados	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-AC-17(2)	Acesso remoto do AC-17(2) | Proteção de confidencialidade e integridade usando criptografia	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(3)	Acesso remoto do AC-17(3) | Pontos de controle de acesso gerenciado	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(4)	Acesso remoto do AC-17(4) | Comandos e acesso privilegiados	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(4)	Acesso remoto do AC-17(4) | Comandos e acesso privilegiados	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17(4)	Acesso remoto do AC-17(4) | Comandos e acesso privilegiados	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.A	Acesso remoto do AC-17.A	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.AA	Acesso remoto do AC-17.AA	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AC-17.B	Acesso remoto do AC-17.B	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.A	Eventos de auditoria do AU-2.A	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.B	Eventos de auditoria do AU-2.B	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.C	Eventos de auditoria do AU-2.C	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-2.D	Eventos de auditoria do AU-2.D	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3(1)	Conteúdo dos registros de auditoria do AU-3(1) | Informações adicionais de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-3.A	Conteúdo dos registros de auditoria do AU-3.A	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-5.A	Resposta a falhas de processamento de auditoria do AU-5.A	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-5.B	Resposta a falhas de processamento de auditoria do AU-5.B	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(1)	Revisão, análise e geração de relatórios de auditoria do AU-6(1) | Integração de processos	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-6(3)	Revisão, análise e relatórios de auditoria do AU-6(3) | Correlacionamento de repositórios de auditoria	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-7(1)	Redução de auditoria e geração de relatórios do AU-7(1) | Processamento automático	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-8.B	Carimbos de data/hora do AU-8.B	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-9(2)	Proteção de informações de auditoria do AU-9(2) | Backup de auditoria em sistemas ou componentes físicos separados	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-AU-9(2)	Proteção de informações de auditoria do AU-9(2) | Backup de auditoria em sistemas ou componentes físicos separados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-9(2)	Proteção de informações de auditoria do AU-9(2) | Backup de auditoria em sistemas ou componentes físicos separados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.
CCCS-fPBMM-AU-9.A	Proteção de informações de auditoria do AU-9.A	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-9.A	Proteção de informações de auditoria do AU-9.A	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-9.A	Proteção de informações de auditoria do AU-9.A	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-AU-11.A	Retenção de registros de auditoria do AU-11.A	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-11.B	Retenção de registros de auditoria do AU-11.B	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-11.C	Retenção de registros de auditoria do AU-11.C	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.A	Geração de auditoria do AU-12.A	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-AU-12.C	Geração de auditoria do AU-12.C	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-3(5)	Interconexões do sistema do CA-3(5) | Restrições nas conexões de rede externas	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.A	Monitoramento contínuo do CA-7.A	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.B	Monitoramento contínuo do CA-7.B	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.C	Monitoramento contínuo do CA-7.C	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.D	Monitoramento contínuo do CA-7.D	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.E	Monitoramento contínuo do CA-7.E	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.F	Monitoramento contínuo do CA-7.F	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	api-gw-xray-enabled	AWS O X-Ray coleta dados sobre as solicitações que seu aplicativo atende e fornece ferramentas que você pode usar para visualizar, filtrar e obter informaçõ es sobre esses dados para identificar problemas e oportunid ades de otimizaçã o. Certifique-se de que o X-Ray esteja ativado para que você possa ver informaçõ es detalhadas não apenas sobre a solicitação e a resposta, mas também sobre as chamadas que seu aplicativ o faz para AWS recursos downstrea m, microsserviços, bancos de dados e APIs HTTP da web.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-7.G	Monitoramento contínuo do CA-7.G	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CA-9.A	Conexões internas do sistema do CA-9.A	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-2.A	Configuração de referência do CM-2.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.A	Controle de alteração de configuração do CM-3.A	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.A	Controle de alteração de configuração do CM-3.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.B	Controle de alteração de configuração do CM-3.B	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.B	Controle de alteração de configuração do CM-3.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.C	Controle de alteração de configuração do CM-3.C	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.C	Controle de alteração de configuração do CM-3.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.D	Controle de alteração de configuração do CM-3.D	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.D	Controle de alteração de configuração do CM-3.D	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.E	Controle de alteração de configuração do CM-3.E	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.E	Controle de alteração de configuração do CM-3.E	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.F	Controle de alteração de configuração do CM-3F	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.F	Controle de alteração de configuração do CM-3F	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.G	Controle de alteração de configuração do CM-3.G	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-3.G	Controle de alteração de configuração do CM-3.G	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscaliza ção e auditoria automatizadas de acesso	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(1)	Restrições de acesso para alterações do CM-5(1) | Fiscalização e auditoria automatizadas de acesso	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5(5)	Restrições de acesso para mudanças CM-5(5) | Limite de produção e privilégios operacionais	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-5.A	Restrições de acesso para alterações do CM-5.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6(1)	Definições de configuração do CM-6(1) | Gerenciamento, aplicação e verificação central automatizados	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6(1)	Definições de configuração do CM-6(1) | Gerenciamento, aplicação e verificação central automatizados	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6(1)	Definições de configuração do CM-6(1) | Gerenciamento, aplicação e verificação central automatizados	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	cmk-backing-key-rotation-enabled	Habilite a alternânc ia de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.A	Definições de configuração do CM-6.A	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	cmk-backing-key-rotation-enabled	Habilite a alternânc ia de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.B	Definições de configuração do CM-6.B	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	cmk-backing-key-rotation-enabled	Habilite a alternânc ia de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.C	Definições de configuração do CM-6.C	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	cmk-backing-key-rotation-enabled	Habilite a alternânc ia de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-6.D	Definições de configuração do CM-6.D	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-7.A	Funcionalidade mínima do CM-7.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-7.A	Funcionalidade mínima do CM-7.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-7.B	Funcionalidade mínima do CM-7.B	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-7.B	Funcionalidade mínima do CM-7.B	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(1)	Inventário de componentes do sistema de informações do CM-8(1) | Atualizações durante instalações ou remoções	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(1)	Inventário de componentes do sistema de informações do CM-8(1) | Atualizações durante instalações ou remoções	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(2)	Inventário de componentes do sistema de informações do CM-8(2) | Manutenção automatizada	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(2)	Inventário de componentes do sistema de informações do CM-8(2) | Manutenção automatizada	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(3)	Inventário de componentes do sistema de informações do CM-8(3) | Detecção automatizada de componentes não autorizados	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(3)	Inventário de componentes do sistema de informações do CM-8(3) | Detecção automatizada de componentes não autorizados	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(3)	Inventário de componentes do sistema de informações do CM-8(3) | Detecção automatizada de componentes não autorizados	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8(3)	Inventário de componentes do sistema de informações do CM-8(3) | Detecção automatizada de componentes não autorizados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.A	Inventário de componentes do sistema de informações do CM-8.A	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.A	Inventário de componentes do sistema de informações do CM-8.A	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.B	Inventário de componentes do sistema de informações do CM-8.B	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.B	Inventário de componentes do sistema de informações do CM-8.B	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.C	Inventário de componentes do sistema de informações do CM-8.C	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.C	Inventário de componentes do sistema de informações do CM-8.C	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.D	Inventário de componentes do sistema de informações do CM-8.D	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.D	Inventário de componentes do sistema de informações do CM-8.D	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.E	Inventário de componentes do sistema de informações do CM-8.E	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CM-8.E	Inventário de componentes do sistema de informações do CM-8.E	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(5)	Plano de contingência do CP-2(5) | Continuar com missões essenciais e funções de negócios	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2(6)	Plano de contingência do CP-2(6) | Local alternativo de processamento ou armazenamento	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.A	Plano de contingência do CP-2.A	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.B	Plano de contingência do CP-2.B	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.C	Plano de contingência do CP-2.C	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.D	Plano de contingência do CP-2.D	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.E	Plano de contingência do CP-2.E	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.F	Plano de contingência do CP-2.F	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-2.G	Plano de contingência do CP-2.G	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(1)	Local de armazenamento alternativo do CP-6(1) | Separação do local primário	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6(2)	Local de armazenamento alternativo do CP-6(2) | Tempos de recuperação e objetivos pontuais	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.A	Local de armazenamento alternativo do CP-6.A	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-6.B	Local de armazenamento alternativo do CP-6.B	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(3)	Backup do sistema de informações do CP-9(3) | Armazenamento separado para informações essenciais	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(7)	Backup do sistema de informações do CP-9(7) | Autorização dupla	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9(7)	Backup do sistema de informações do CP-9(7) | Autorização dupla	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.A	Backup do sistema de informações do CP-9.A	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.AA	Backup do sistema de informações do CP-9.B	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.B	Backup do sistema de informações do CP-9.C	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.C	Backup do sistema de informações do CP-9.D	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-9.D	Backup do sistema de informações do CP-9.E	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informaçõ es do CP-10.A	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informaçõ es do CP-10.A	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informaçõ es do CP-10.A	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-CP-10.A	Recuperação e reconstituição do sistema de informações do CP-10.A	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(1)	Identificação e autenticação do IA-2(1) (usuários organizacionais) | Acesso de rede a contas privilegiadas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(1)	Identificação e autenticação do IA-2(1) (usuários organizacionais) | Acesso de rede a contas privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(1)	Identificação e autenticação do IA-2(1) (usuários organizacionais) | Acesso de rede a contas privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(3)	Identificação e autenticação do IA-2(3) (usuários organizacionais) | Acesso local a contas privilegiadas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(3)	Identificação e autenticação do IA-2(3) (usuários organizacionais) | Acesso local a contas privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(3)	Identificação e autenticação do IA-2(3) (usuários organizacionais) | Acesso local a contas privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(8)	Identificação e autenticação do IA-2(8) (usuários organizacionais) | Acesso de rede a contas privilegiadas: resistente à repetição	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(8)	Identificação e autenticação do IA-2(8) (usuários organizacionais) | Acesso de rede a contas privilegiadas: resistente à repetição	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(8)	Identificação e autenticação do IA-2(8) (usuários organizacionais) | Acesso de rede a contas privilegiadas: resistente à repetição	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(11)	Identificação e autenticação do IA-2(11) (usuários organizacionais) | Acesso remoto: dispositivo separado	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(11)	Identificação e autenticação do IA-2(11) (usuários organizacionais) | Acesso remoto: dispositivo separado	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2(11)	Identificação e autenticação do IA-2(11) (usuários organizacionais) | Acesso remoto: dispositivo separado	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2.A	Identificação e autenticação do IA-2.A (usuários organizacionais)	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2.A	Identificação e autenticação do IA-2.A (usuários organizacionais)	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2.A	Identificação e autenticação do IA-2.A (usuários organizacionais)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-2.A	Identificação e autenticação do IA-2.A (usuários organizacionais)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4(4)	Gerenciamento de identificadores do IA-4(4) | Identificação do status do usuário	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.A	Gerenciamento de identificadores do IA-4.A	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.A	Gerenciamento de identificadores do IA-4.A	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.A	Gerenciamento de identificadores do IA-4.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.B	Gerenciamento de identificadores do IA-4.B	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.B	Gerenciamento de identificadores do IA-4.B	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.B	Gerenciamento de identificadores do IA-4.B	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.C	Gerenciamento de identificadores do IA-4.C	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.C	Gerenciamento de identificadores do IA-4.C	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.C	Gerenciamento de identificadores do IA-4.C	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.D	Gerenciamento de identificadores do IA-4.D	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.D	Gerenciamento de identificadores do IA-4.D	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.D	Gerenciamento de identificadores do IA-4.D	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.E	Gerenciamento de identificadores do IA-4.E	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.E	Gerenciamento de identificadores do IA-4.E	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-4.E	Gerenciamento de identificadores do IA-4.E	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(1)	Gerenciamento de autenticadores do IA-5(1) | Autenticação baseada em senha	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(2)	Gerenciamento de autenticadores do IA-5(2) | Autenticação baseada em PKI	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
CCCS-fPBMM-IA-5(2)	Gerenciamento de autenticadores do IA-5(2) | Autenticação baseada em PKI	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(4)	Gerenciamento de autenticadores do IA-5(4) | Suporte automatizado para determinação do nível de segurança de senha	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(8)	Gerenciamento de autenticadores do IA-5(8) | Várias contas do sistema de informações	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(8)	Gerenciamento de autenticadores do IA-5(8) | Várias contas do sistema de informações	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5(8)	Gerenciamento de autenticadores do IA-5(8) | Várias contas do sistema de informações	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.A	Gerenciamento de autenticadores do IA-5.A	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.A	Gerenciamento de autenticadores do IA-5.A	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.A	Gerenciamento de autenticadores do IA-5.A	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.A	Gerenciamento de autenticadores do IA-5.A	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.B	Gerenciamento de autenticadores do IA-5.B	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.B	Gerenciamento de autenticadores do IA-5.B	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.B	Gerenciamento de autenticadores do IA-5.B	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.B	Gerenciamento de autenticadores do IA-5.B	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.C	Gerenciamento de autenticadores do IA-5.C	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.C	Gerenciamento de autenticadores do IA-5.C	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.C	Gerenciamento de autenticadores do IA-5.C	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.C	Gerenciamento de autenticadores do IA-5.C	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.D	Gerenciamento de autenticadores do IA-5.D	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.D	Gerenciamento de autenticadores do IA-5.D	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.D	Gerenciamento de autenticadores do IA-5.D	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.D	Gerenciamento de autenticadores do IA-5.D	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-IA-5.e	Gerenciamento de autenticadores do IA-5.E	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-IA-5.e	Gerenciamento de autenticadores do IA-5.E	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-IA-5.e	Gerenciamento de autenticadores do IA-5.E	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-FPBMM-IA-5.e	Gerenciamento de autenticadores do IA-5.E	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.F	Gerenciamento de autenticadores do IA-5.F	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.F	Gerenciamento de autenticadores do IA-5.F	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.F	Gerenciamento de autenticadores do IA-5.F	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.F	Gerenciamento de autenticadores do IA-5.F	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.G	Gerenciamento de autenticadores do IA-5.G	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.G	Gerenciamento de autenticadores do IA-5.G	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.G	Gerenciamento de autenticadores do IA-5.G	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.G	Gerenciamento de autenticadores do IA-5.G	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.H	Gerenciamento de autenticadores do IA-5.H	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.H	Gerenciamento de autenticadores do IA-5.H	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.H	Gerenciamento de autenticadores do IA-5.H	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.H	Gerenciamento de autenticadores do IA-5.H	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.I	Gerenciamento de autenticadores do IA-5.I	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.I	Gerenciamento de autenticadores do IA-5.I	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.I	Gerenciamento de autenticadores do IA-5.I	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.I	Gerenciamento de autenticadores do IA-5.I	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.J	Gerenciamento de autenticadores do IA-5.J	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.J	Gerenciamento de autenticadores do IA-5.J	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.J	Gerenciamento de autenticadores do IA-5.J	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IA-5.J	Gerenciamento de autenticadores do IA-5.J	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-IR-6(1)	Relatório de incidentes do IR-6(1) | Geração automatizada de relatórios	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-3.A	Ferramentas de manutenção do MA-3.A	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-3.A	Ferramentas de manutenção do MA-3.A	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MA-4(1)	Manutenção não local do MA-4(1) | Auditoria e análise	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-MP-2.A	Acesso à mídia do MP-2.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-RA-5.A	Verificação de vulnerabilidades do RA-5.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-RA-5.B	Verificação de vulnerabilidades do RA-5.B	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-RA-5.C	Verificação de vulnerabilidades do RA-5.C	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-RA-5.D	Verificação de vulnerabilidades do RA-5.D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-RA-5.E	Verificação de vulnerabilidades do RA-5.E	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SA-10(1)	Gerenciamento de configuração para desenvolvedores do SA-10(1) | Verificação de integridade de software e firmware	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-5.A	Proteção contra negação de serviço do SC-5.A	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-5.A	Proteção contra negação de serviço do SC-5.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-6.A	Disponibilidade de recursos do SC-6.A	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-SC-7(3)	Proteção de limites do SC-7(3) | Pontos de acesso	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(4)	Proteção de limites do SC-7(4) | Serviços externos de telecomunicações	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(5)	Proteção de limites do SC-7(5) | Negação por padrão e permissão por exceção	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(5)	Proteção de limites do SC-7(5) | Negação por padrão e permissão por exceção	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(5)	Proteção de limites do SC-7(5) | Negação por padrão e permissão por exceção	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(5)	Proteção de limites do SC-7(5) | Negação por padrão e permissão por exceção	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7(7)	Proteção de limite do SC-7(7) | Prevenção de tunelamento dividido em dispositivos remotos	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.A	Proteção de limites do SC-7.A	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.B	Proteção de limites do SC-7.B	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-7.C	Proteção de limites do SC-7.C	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8(1)	Confidencialidade e integridade de transmissão do SC-8(1) | Proteção física criptográfica ou alternativa	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-8.A	Confidencialidade e integridade de transmissão do SC-8.A	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-12(1)	Estabelecimento e gerenciamento de chaves criptográficas do SC-12(1) | Disponibilidade	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
CCCS-fPBMM-SC-12(2)	Estabelecimento e gerenciamento de chaves criptográficas do SC-12(2) | Chaves simétricas	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-12(2)	Estabelecimento e gerenciamento de chaves criptográficas do SC-12(2) | Chaves simétricas	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
CCCS-fPBMM-SC-12.A	Estabelecimento e gerenciamento de chaves criptográficas do SC-12.A	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-12.A	Estabelecimento e gerenciamento de chaves criptográficas do SC-12.A	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-13.A	Proteção criptográfica do SC-13.A	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-22.A	Arquitetura e provisionamento para serviço de resolução de nomes e endereços do SC-22.A	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-23.A	Autenticidade de sessão do SC-23.A	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28(1)	Proteção de informações em repouso SC-28(1) | Proteção criptográfica	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SC-28.A	Proteção de informações em repouso do SC-28.A	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(2)	Correção de falhas do SI-2(2) | Status automatizado de correção de falhas	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2(3)	Correção de falhas do SI-2(3) | Tempo para correção de falhas benchmarks para ações corretivas	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.A	Correção de falhas do SI-2.A	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.B	Correção de falhas do SI-2.B	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.C	Correção de falhas do SI-2.C	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-2.D	Correção de falhas do SI-2.D	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3(1)	Proteção contra códigos mal-intencionados do SI-3(1) | Gerenciamento central	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3(7)	Proteção contra códigos mal-intencionados do SI-3(7) | Detecção não baseada em assinatura	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.A	Proteção contra códigos mal-intencionados do SI-3.A	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.A	Proteção contra códigos mal-intencionados do SI-3.A	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.A	Proteção contra códigos mal-intencionados do SI-3.A	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.A	Proteção contra códigos mal-intencionados do SI-3.A	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.A	Proteção contra códigos mal-intencionados do SI-3.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.B	Proteção contra códigos mal-intencionados do SI-3.B	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.B	Proteção contra códigos mal-intencionados do SI-3.B	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.B	Proteção contra códigos mal-intencionados do SI-3.B	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.B	Proteção contra códigos mal-intencionados do SI-3.B	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.C	Proteção contra códigos mal-intencionados do SI-3.C	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.C	Proteção contra códigos mal-intencionados do SI-3.C	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.C	Proteção contra códigos mal-intencionados do SI-3.C	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.C	Proteção contra códigos mal-intencionados do SI-3.C	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.D	Proteção contra códigos mal-intencionados do SI-3.D	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.D	Proteção contra códigos mal-intencionados do SI-3.D	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.D	Proteção contra códigos mal-intencionados do SI-3.D	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-3.D	Proteção contra códigos mal-intencionados do SI-3.D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(1)	Monitoramento do sistema de informaçõ es do SI-4(1) | Sistema de detecção de invasões em todo o sistema	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(1)	Monitoramento do sistema de informações do SI-4(1) | Sistema de detecção de invasões em todo o sistema	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(2)	Monitoramento do sistema de informações do SI-4(2) | Ferramentas automatizadas para análise em tempo real	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(2)	Monitoramento do sistema de informações do SI-4(2) | Ferramentas automatizadas para análise em tempo real	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(4)	Monitoramento do sistema de informações do SI-4(4) | Tráfego de comunicações de entrada e saída	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(4)	Monitoramento do sistema de informações do SI-4(4) | Tráfego de comunicações de entrada e saída	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(5)	Monitoramento do sistema de informaçõ es do SI-4(5) | Alertas gerados pelo sistema	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(11)	Monitoramento do sistema de informações do SI-4(11) | Análise de anomalias no tráfego de comunicações	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(11)	Monitoramento do sistema de informações do SI-4(11) | Análise de anomalias no tráfego de comunicações	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(16)	Monitoramento do sistema de informações do SI-4(16) | Correlação de informações de monitoramento	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(16)	Monitoramento do sistema de informações do SI-4(16) | Correlação de informações de monitoramento	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(20)	Monitoramento do sistema de informações do SI-4(20) | Usuário privilegiado	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(23)	Monitoramento do sistema de informaçõ es do SI-4(23) | Dispositivos baseados em host	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4(23)	Monitoramento do sistema de informações do SI-4(23) | Dispositivos baseados em host	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.A	Monitoramento do sistema de informações do SI-4.A	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.A	Monitoramento do sistema de informaçõ es do SI-4.A	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.A	Monitoramento do sistema de informações do SI-4.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.A	Monitoramento do sistema de informações do SI-4.A	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.A	Monitoramento do sistema de informaçõ es do SI-4.A	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.B	Monitoramento do sistema de informaçõ es do SI-4.B	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.B	Monitoramento do sistema de informaçõ es do SI-4.B	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.B	Monitoramento do sistema de informações do SI-4.B	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.B	Monitoramento do sistema de informações do SI-4.B	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.B	Monitoramento do sistema de informações do SI-4.B	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.C	Monitoramento do sistema de informações do SI-4.C	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.C	Monitoramento do sistema de informaçõ es do SI-4.C	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.C	Monitoramento do sistema de informações do SI-4.C	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.C	Monitoramento do sistema de informações do SI-4.C	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.C	Monitoramento do sistema de informações do SI-4.C	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.D	Monitoramento do sistema de informaçõ es do SI-4.D	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.D	Monitoramento do sistema de informações do SI-4.D	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.D	Monitoramento do sistema de informações do SI-4.D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.D	Monitoramento do sistema de informações do SI-4.D	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.D	Monitoramento do sistema de informações do SI-4.D	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.E	Monitoramento do sistema de informações do SI-4.E	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.E	Monitoramento do sistema de informaçõ es do SI-4.E	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.E	Monitoramento do sistema de informações do SI-4.E	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.E	Monitoramento do sistema de informações do SI-4.E	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.E	Monitoramento do sistema de informações do SI-4.E	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.F	Monitoramento do sistema de informaçõ es do SI-4.F	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.F	Monitoramento do sistema de informaçõ es do SI-4.F	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.F	Monitoramento do sistema de informações do SI-4.F	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.F	Monitoramento do sistema de informações do SI-4.F	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.F	Monitoramento do sistema de informações do SI-4.F	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.G	Monitoramento do sistema de informações do SI-4.G	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.G	Monitoramento do sistema de informaçõ es do SI-4.G	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.G	Monitoramento do sistema de informações do SI-4.G	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CCCS-fPBMM-SI-4.G	Monitoramento do sistema de informações do SI-4.G	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-4.G	Monitoramento do sistema de informações do SI-4.G	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-5.A	Alertas, recomendações e diretrizes de segurança do SI-5.A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-5.B	Alertas, recomendações e diretrizes de segurança do SI-5.B	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-5.C	Alertas, recomendações e diretrizes de segurança do SI-5.C	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-5.D	Alertas, recomendações e diretrizes de segurança do SI-5.D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-7(1)	Integridade de software, firmware e informações do SI-7(1) | Verificações de integridade	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-7(7)	Software, firmware e integridade das informações do SI-7(7) | Integraçã o de detecção e resposta	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-7.A	Software, firmware e integridade de informações do SI-7.A	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CCCS-fPBMM-SI-12.A	Tratamento e retenção de informações do SI-12.A	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o perfil de controle de nuvem média do Centro Canadense de Segurança Cibernética (CCCS).

Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 1 e as regras de AWS Config/Verificações de processo gerenciadas.AWS Config Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CIS Amazon Web Services Foundation v1.4 Nível 1. Um controle do CIS Amazon Web Services Foundation v1.4 Nível 1 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Para obter mais informações sobre verificações de processo, consulte process-checks.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Manter detalhes de contato atuais	account-contact-details-configured (verificação do processo)	Atualize o e-mail de contato e o número de telefone das contas da AWS e mapeie-os para mais de uma pessoa na sua organização. Na seção Minha conta do console, verifique se as informaçõ es corretas estão especificadas na seção Informaçõ es de contato. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			amazon_web_services/
1.2	Verificar se as informações de contato de segurança estão registradas	account-security-contact-configured (Verificação do processo)	Atualize o e-mail de contato e o número de telefone da equipe de segurança da sua organização. Na seção Minha conta do AWS Management Console, certifique-se de que as informações corretas sejam especificadas na seção Segurança. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.4	Verificar se não existe uma chave de acesso do usuário 'raiz'	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.5	Verificar se a MFA está habilitada para o usuário 'raiz'	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,7	Eliminar o uso do usuário 'raiz' para tarefas administr ativas e diárias	root-account-regular-use (Verificação do processo)	O uso da conta raiz deve ser evitado nas tarefas diárias. No IAM, execute um relatório de credencia l para examinar quando o usuário raiz foi usado pela última vez. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.8	Verificar se a política de senha do IAM exige um comprimento mínimo de 14 ou mais	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.9	Verificar se a política de senha do IAM impede a reutilização de senhas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.10	Verificar se a autenticação multifator (MFA) está ativada para todos os usuários que têm uma senha do console	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.11	Não configurar chaves de acesso durante a configura ção inicial do usuário para todos os usuários que têm uma senha do console	iam-user-console-a nd- (Verificação do processo) api-access-at-creation	Não configure chaves de acesso durante a configuração inicial do usuário para os usuários que têm uma senha do console. Para todos os usuários com acesso ao console, compare a 'Hora de criação' do usuário com a data da chave de acesso 'Criada'. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.12	Verificar se as credenciais não usadas por 45 dias ou mais são desativadas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor para a maxCredentialUsageIdade (valor padrão CIS: 45). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.13	Verificar se há apenas uma chave de acesso ativa disponível para cada usuário	iam- user-single-access-key (Verificação do processo)	Verifique se há apenas uma chave de acesso ativa disponível para cada usuário. Para todos os usuários, verifique se há apenas uma chave ativa usada na guia Credenciais de segurança para cada usuário no IAM. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.14	Verificar se as chaves de acesso são alternadas a cada 90 dias ou menos	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.16	Verificar se as políticas do IAM que permitem privilégios administrativos "*:*" completos não estão anexadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.17	Garanta que uma função de suporte tenha sido criada para gerenciar incidentes com AWS o Support	iam-policy-in-use	AWS O Identity and Access Managemen t (IAM) pode ajudar você a gerenciar permissões e autorizações de acesso, garantindo que as políticas do IAM sejam atribuídas aos usuários, funções ou grupos apropriad os. A restrição dessas políticas também incorpora os princípio s do privilégio mínimo e separação de deveres. Essa regra exige que você defina o PolicYarn como arn:aws:iam: :aws:poli cy/, para gerenciam ento de incidente s com o Support. AWSSupportAccess AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,19	Verificar se todos os certificados SSL/TLS expirados armazenados no AWS IAM são removidos	iam-expired-certificates (Verificação do processo)	Verifique se todos os certificados SSL/TLS expirados armazenados no IAM são removidos. Na linha de comando com a AWS CLI instalada, execute o comando 'AWS iam list-server-certificates' e determine se há algum certificado de servidor expirado. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,20	Certifique-se de que o AWS IAM Access Analyzer esteja ativado	iam-access-analyzer-enabled (Verificação do processo)	Verifique se o IAM Access Analyzer está habilitado. Na seção IAM do console, selecione Access Analyzer e verifique se o STATUS está definido como Ativo. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.3	Verificar se a Exclusão de MFA está ativada nos buckets do S3	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Adicionar a exclusão de autenticação multifator (MFA) a um bucket do S3 requer um fator adicional de autenticação para alterar o estado da versão do seu bucket ou excluir uma versão do objeto. A exclusão da MFA pode adicionar uma camada adicional de segurança caso as credenciais de segurança sejam comprometidas ou o acesso não autorizado seja concedido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.5	Verificar se os buckets do S3 estão configurados com 'Bloqueio de acesso público (configur ações do bucket)'	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.5	Verificar se os buckets do S3 estão configurados com 'Bloqueio de acesso público (configur ações do bucket)'	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
2.2.1	Verificar se a criptografia de volume do EBS está habilitad a	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para seus volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.1	Verificar se a criptografia de volume do EBS está habilitada	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
2.3.1	Verificar se a criptografia está habilitada para instâncias do RDS	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.3.1	Verificar se a criptografia está habilitada para instâncias do RDS	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	O Ensure CloudTrail está ativado em todas as regiões	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
3.4	Garanta que as CloudTrail trilhas sejam integradas aos CloudWatch registros	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6	Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Verificar se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas	alarm-unauthorized-api-calls (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.2	Verificar se existe um alarme e um filtro de métrica de log para login do Management Console sem MFA	alarm- sign-in-without-mfa (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para login no AWS Management Console sem autenticação multifator (MFA). Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3	Verificar se existe um alarme e um filtro de métrica de log para uso da conta "raiz"	alarm-root-account-use (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para uso da conta "raiz". Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do IAM	alarm-iam-policy-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações de política do IAM. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.5	Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração	alarm-cloudtrail-config-change (Verificação do processo)	Certifique-se de que exista um filtro métrico de log e um alarme para alterações na AWS CloudTrail configuração. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3	alarm-s3- bucket-policy-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.12	Verificar se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede	alarm- vpc-network-gateway-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.13	Verificar se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas	alarm- vpc-route-table-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.14	Verificar se existe um alarme e um filtro de métrica de log para alterações de VPC	alarm-vpc-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações no Amazon Virtual Private Cloud (VPC). Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.15	Verificar se existe um alarme e um filtro de métrica de log para alterações do AWS Organizations	alarm-organizations-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações do AWS Organizations. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.1	Verificar se nenhum ACLs de rede permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	nacl-no-unrestricted-ssh-rdp	Verifique se nenhum ACLs de rede permite o ingresso público às portas de administração do servidor remoto. Na seção VPC do console, verifique se há ACLs de rede com uma fonte de '0.0.0.0/0' com portas permitidas ou intervalos de portas, incluindo portas de administração do servidor remoto. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Verificar se nenhum grupo de segurança permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Verificar se nenhum grupo de segurança permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (valor padrão CIS: 3389). Os valores reais devem refletir as políticas da organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1.

Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Center for Internet Security (CIS) Amazon Web Services Foundation v1.4 Level 2 e as regras de AWS Config/Verificações de processo gerenciadas.AWS Config Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CIS Amazon Web Services Foundation v1.4 Nível 2. Um controle do CIS Amazon Web Services Foundation v1.4 Nível 2 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Para obter mais informações sobre verificações de processo, consulte process-checks.

Região da AWS: Regiões da AWS em todos os lugares onde há suporte para pacotes de conformidade (suporte regional), exceto (Leste dos EUA), AWS GovCloud (Oeste dos EUA) e Oriente Médio AWS GovCloud (Bahrein)

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Manter detalhes de contato atuais	account-contact-details-configured (verificação do processo)	Atualize o e-mail de contato e o número de telefone das contas da AWS e mapeie-os para mais de uma pessoa na sua organização. Na seção Minha conta do console, verifique se as informaçõ

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			es corretas estão especificadas na seção Informaçõ es de contato. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2	Verificar se as informações de contato de segurança estão registradas	account-security-contact-configured (Verificação do processo)	Atualize o e-mail de contato e o número de telefone da equipe de segurança da sua organização. Na seção Minha conta do AWS Management Console, certifique-se de que as informações corretas sejam especificadas na seção Segurança. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.4	Verificar se não existe uma chave de acesso do usuário 'raiz'	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.5	Verificar se a MFA está habilitada para o usuário 'raiz'	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.6	Verificar se a MFA de hardware está habilitada para a conta do usuário 'raiz'	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,7	Eliminar o uso do usuário 'raiz' para tarefas administr ativas e diárias	root-account-regular-use (Verificação do processo)	O uso da conta raiz deve ser evitado nas tarefas diárias. No IAM, execute um relatório de credencia l para examinar quando o usuário raiz foi usado pela última vez. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.8	Verificar se a política de senha do IAM exige um comprimento mínimo de 14 ou mais	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.9	Verificar se a política de senha do IAM impede a reutilização de senhas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.10	Verificar se a autenticação multifator (MFA) está ativada para todos os usuários que têm uma senha do console	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.11	Não configurar chaves de acesso durante a configuração inicial do usuário para todos os usuários que têm uma senha do console	iam-user-console-and- (Verificação do processo) api-access-at-creation	Não configure chaves de acesso durante a configuração inicial do usuário para os usuários que têm uma senha do console. Para todos os usuários com acesso ao console, compare a 'Hora de criação' do usuário com a data da chave de acesso 'Criada'. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.12	Verificar se as credenciais não usadas por 45 dias ou mais são desativadas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor para a maxCredentialUsageIdade (valor padrão CIS: 45). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.13	Verificar se há apenas uma chave de acesso ativa disponível para cada usuário	iam- user-single-access-key (Verificação do processo)	Verifique se há apenas uma chave de acesso ativa disponível para cada usuário. Para todos os usuários, verifique se há apenas uma chave ativa usada na guia Credenciais de segurança para cada usuário no IAM. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.14	Verificar se as chaves de acesso são alternadas a cada 90 dias ou menos	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.15	Garantir que os usuários recebam permissões somente por meio de grupos	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.16	Verificar se as políticas do IAM que permitem privilégios administrativos "*:*" completos não estão anexadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.17	Garanta que uma função de suporte tenha sido criada para gerenciar incidentes com AWS o Support	iam-policy-in-use	AWS O Identity and Access Managemen t (IAM) pode ajudar você a gerenciar permissões e autorizações de acesso, garantindo que as políticas do IAM sejam atribuídas aos usuários, funções ou grupos apropriad os. A restrição dessas políticas também incorpora os princípio s do privilégio mínimo e separação de deveres. Essa regra exige que você defina o PolicYarn como arn:aws:iam: :aws:poli cy/, para gerenciam ento de incidente s com o Support. AWSSupportAccess AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,18	Certifique-se de que as funções de instância do IAM sejam usadas para acesso a AWS recursos a partir de instâncias	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,19	Verificar se todos os certificados SSL/TLS expirados armazenados no AWS IAM são removidos	iam-expired-certificates (Verificação do processo)	Verifique se todos os certificados SSL/TLS expirados armazenados no IAM são removidos. Na linha de comando com a AWS CLI instalada, execute o comando 'AWS iam list-server-certificates' e determine se há algum certificado de servidor expirado. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,20	Certifique-se de que o AWS IAM Access Analyzer esteja ativado	iam-access-analyzer-enabled (Verificação do processo)	Verifique se o IAM Access Analyzer está habilitado. Na seção IAM do console, selecione Access Analyzer e verifique se o STATUS está definido como Ativo. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1,21	Garanta que os usuários sejam gerenciados centralmente por meio da federação de identidades ou do AWS Organizations para ambientes com várias contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
2.1.1	Garanta que todos os buckets S3 funcionem encryption-at-rest	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.2	Verificar se a política de bucket do S3 está configurada para negar solicitações HTTP	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.3	Verificar se a Exclusão de MFA está ativada nos buckets do S3	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Adicionar a exclusão de autentica ção multifator (MFA) a um bucket do S3 requer um fator adicional de autentica ção para alterar o estado da versão do seu bucket ou excluir uma versão do objeto. A exclusão da MFA pode adicionar uma camada adicional de segurança caso as credenciais de segurança sejam comprometidas ou o acesso não autorizad o seja concedido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.5	Verificar se os buckets do S3 estão configurados com 'Bloqueio de acesso público (configur ações do bucket)'	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1.5	Verificar se os buckets do S3 estão configurados com 'Bloqueio de acesso público (configurações do bucket)'	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
2.2.1	Verificar se a criptografia de volume do EBS está habilitada	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.1	Verificar se a criptografia de volume do EBS está habilitad a	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
2.3.1	Verificar se a criptografia está habilitada para instâncias do RDS	rds-snapshot-encrypted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.3.1	Verificar se a criptografia está habilitada para instâncias do RDS	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	O Ensure CloudTrail está ativado em todas as regiões	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2	Certifique-se de que a validação do arquivo de CloudTrail log esteja ativada	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Certifique-se de que o bucket do S3 usado para armazenar CloudTrail registros não esteja acessível ao público	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
3.4	Garanta que as CloudTrail trilhas sejam integradas aos CloudWatch registros	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Certifique-se de que o AWS Config esteja ativado em todas as regiões	config-enabled-all-regions (Verificação do processo)	Certifique-se de que o AWS Config esteja ativado em todas as AWS regiões. Na seção AWS Config do console, para cada região ativada, certifique-se de que o gravador AWS Config esteja configura do corretamente. Verifique se o registro de recursos globais da AWS está ativado em pelo menos uma região. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6	Certifique-se de que o registro de acesso ao bucket do S3 esteja ativado no bucket do CloudTrail S3	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.7	Garanta que CloudTrail os registros sejam criptografados em repouso usando CMKs do KMS	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
3.8	Verificar se a alternância para CMKs criadas pelo cliente está habilitada	cmk-backing-key-ro tation-enabled	Habilite a alternânc ia de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.9	Verificar se o registro em log do fluxo da VPC está habilitado em todas as VPCs	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
3.10	Verificar se o registro em log no nível do objeto para eventos de gravação está habilitado para o bucket S3	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Verificar se o registro em log no nível do objeto para eventos de leitura está habilitado para o bucket S3	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
4.1	Verificar se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas	alarm-unauthorized-api-calls (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para chamadas de API não autorizadas Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.2	Verificar se existe um alarme e um filtro de métrica de log para login do Management Console sem MFA	alarm- sign-in-without-mfa (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para login no AWS Management Console sem autenticação multifator (MFA). Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3	Verificar se existe um alarme e um filtro de métrica de log para uso da conta "raiz"	alarm-root-account-use (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para uso da conta "raiz". Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do IAM	alarm-iam-policy-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações de política do IAM. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.5	Certifique-se de que exista um filtro métrico de registro e um alarme para alterações CloudTrail de configuração	alarm-cloudtrail-config-change (Verificação do processo)	Certifique-se de que exista um filtro métrico de log e um alarme para alterações na AWS CloudTrail configuração. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Verificar se existe um alarme e um filtro de métrica de log para falhas de autentica ção do AWS Manag ement Console	alarm-console-auth-failures (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para falhas de autentica ção do AWS Manag ement Console. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.7	Verificar se existe um alarme e um filtro de métrica de log para a desativação ou exclusão programada de CMKs criadas pelo cliente	alarm-kms- disable-or-delete-cmk (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para a desativação ou exclusão programada de CMKs criadas pelo cliente. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8	Verificar se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3	alarm-s3- bucket-policy-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações de política do bucket do S3. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4,9	Certifique-se de que exista um filtro métrico de log e um alarme para alterações na AWS configuração do Config	alarm-aws-config-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações de configuração do AWS Config. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.10	Verificar se existe um alarme e um filtro de métrica de log para alterações do grupo de segurança	alarm- vpc-secri ty-group-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações do grupo de segurança. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.11	Verificar se existe um alarme e um filtro de métrica de log para alterações em listas de controle de acesso à rede (NACL)	alarm-vpc-nacl-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações em listas de controle de acesso à rede (NACL). Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.12	Verificar se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede	alarm- vpc-network-gateway-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações nos gateways de rede. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.13	Verificar se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas	alarm- vpc-route-table-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações da tabela de rotas. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.14	Verificar se existe um alarme e um filtro de métrica de log para alterações de VPC	alarm-vpc-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações no Amazon Virtual Private Cloud (VPC). Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.15	Verificar se existe um alarme e um filtro de métrica de log para alterações do AWS Organizations	alarm-organizations-change (Verificação do processo)	Verifique se existe um alarme e um filtro de métrica de log para alterações do AWS Organizations. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.1	Verificar se nenhum ACLs de rede permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	nacl-no-unrestricted-ssh-rdp	Verifique se nenhum ACLs de rede permite o ingresso público às portas de administração do servidor remoto. Na seção VPC do console, verifique se há ACLs de rede com uma fonte de '0.0.0.0/0' com portas permitidas ou intervalos de portas, incluindo portas de administração do servidor remoto. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundations Benchmark versão 1.4.0, disponível em https://www.cisecurity.org/benchmark/amazon_web_services/

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Verificar se nenhum grupo de segurança permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Verificar se nenhum grupo de segurança permite o ingresso de 0.0.0.0/0 às portas de administração do servidor remoto	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (valor padrão CIS: 3389). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.3	Verificar se o grupo de segurança padrão de cada VPC restringe todo o tráfego	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Verificar se as tabelas de rotas para o emparelhamento de VPCs sejam de "acesso mínimo"	vpc-peering-least-access (Verificação do processo)	Verifique se as tabelas de rotas para o emparelhamento de Amazon VPC sejam de "acesso mínimo". Na seção VPC do console, examine as entradas da tabela de rotas para garantir que o menor número de sub-redes ou hosts necessári os para cumprir a finalidade do peering seja roteável. Para obter mais detalhes sobre a auditoria desse controle, consulte o documento CIS Amazon Web Services Foundatio ns Benchmark versão 1.4.0, disponível em https://www.cisecu rity.org/benchmark/ amazon_web_servic es/

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2.

Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG1

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Center for Internet Security (CIS) Critical Security Controls v8 IG1 e as regras gerenciadas do AWS Config. Cada um AWS Config se aplica a um AWS recurso específico e está relacionado a um ou mais controles CIS Critical Security Controls v8 IG1. Um controle do CIS Critical Security Controls v8 IG1 pode estar relacionado a várias regras do AWS Config . Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	vpc-network-acl-un used-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-security-group-attached-to-eni	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
2.2	Verificar se o software autorizado tem suporte atualmente	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
3.3	Configurar listas de controle de acesso a dados	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.3	Configurar listas de controle de acesso a dados	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
3.3	Configurar listas de controle de acesso a dados	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.3	Configurar listas de controle de acesso a dados	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.3	Configurar listas de controle de acesso a dados	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de controle de acesso a dados	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
3.4	Aplicar a retenção de dados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Aplicar a retenção de dados	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
4.1	Estabelecer e manter um processo de configuração seguro	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
4.1	Estabelecer e manter um processo de configuração seguro	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporativos com segurança	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporativos com segurança	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporativos com segurança	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
4.6	Gerenciar ativos e softwares corporativos com segurança	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporativos com segurança	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporativos com segurança	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.7	Gerenciar contas padrão em ativos e software corporativos	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
5.1	Estabelecer e manter um inventário de contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.3	Desabilitar contas inativas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.5	Exigir MFA para acesso administrativo	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Estabelecer e manter um processo de gerenciamento de logs de auditoria	audit-log-policy-exists (Verificação do processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.
8.2	Coletar logs de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
8.2	Coletar logs de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
8.2	Coletar logs de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
8.3	Garantir o armazenamento adequado dos logs de auditoria	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implantar e manter um software antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2	Configurar atualizações automáticas de assinatura antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.2	Fazer backups automatizados	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
11.3	Proteger os dados de recuperação	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger os dados de recuperação	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para controles críticos de segurança do CIS v8 IG1.

Práticas recomendadas operacionais para o CIS Critical Security Controls v8 IG2

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Center for Internet Security (CIS) Critical Security Controls v8 IG2 e as regras gerenciadas do AWS Config. Cada um AWS Config se aplica a um AWS

recurso específico e está relacionado a um ou mais controles CIS Critical Security Controls v8 IG2. Um controle do CIS Critical Security Controls v8 IG2 pode estar relacionado a várias regras do AWS Config . Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			padrões da organizaç ão.
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	vpc-network-acl-un used-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-security-group-attached-to-eni	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
2.2	Verificar se o software autorizado tem suporte atualmente	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrad o um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataform a. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataform a.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Utilizar ferramentas automatizadas de inventário de software	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Utilizar ferramentas automatizadas de inventário de software	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
3.3	Configurar listas de controle de acesso a dados	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.3	Configurar listas de controle de acesso a dados	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
3.3	Configurar listas de controle de acesso a dados	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.3	Configurar listas de controle de acesso a dados	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.3	Configurar listas de controle de acesso a dados	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de controle de acesso a dados	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
3.4	Aplicar a retenção de dados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Aplicar a retenção de dados	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
3.10	Criptografar dados confidenciais em trânsito	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.10	Criptografar dados confidenciais em trânsito	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
3.11	Criptografar dados confidenciais em repouso	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
3.11	Criptografar dados confidenciais em repouso	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
4.1	Estabelecer e manter um processo de configuração seguro	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
4.1	Estabelecer e manter um processo de configuração seguro	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporati vos com segurança	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporati vos com segurança	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporati vos com segurança	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
4.6	Gerenciar ativos e softwares corporati vos com segurança	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporativos com segurança	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporativos com segurança	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.7	Gerenciar contas padrão em ativos e software corporativos	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
5.1	Estabelecer e manter um inventário de contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.3	Desabilitar contas inativas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6	Centralizar o gerenciamento de contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.5	Exigir MFA para acesso administrativo	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.7	Centralizar o controle de acesso	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7,5	Executar verificações automatizadas de vulnerabilidades de ativos corporativos internos	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.
8.1	Estabelecer e manter um processo de gerenciamento de logs de auditoria	audit-log-policy-exists (Verificação do processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
8.2	Coletar logs de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
8.2	Coletar logs de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
8.3	Garantir o armazenamento adequado dos logs de auditoria	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
8.5	Coletar logs de auditoria detalhados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
8.5	Coletar logs de auditoria detalhados	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.7	Coletar logs de auditoria de solicitaç ões de URL	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.
8.9	Centralizar os logs de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.10	Reter logs de auditoria	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
8.10	Reter logs de auditoria	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implantar e manter um software antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2	Configurar atualizações automáticas de assinatura antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.4	Configurar a verificação antimalware automática de mídia removível	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.6	Gerenciar centralmente o software antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.7	Usar um software antimalware baseado em comportamento	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.2	Fazer backups automatizados	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
11.3	Proteger os dados de recuperação	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger os dados de recuperação	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
12.2	Estabelecer e manter uma arquitetura de rede segura	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
12.2	Estabelecer e manter uma arquitetura de rede segura	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
12.2	Estabelecer e manter uma arquitetura de rede segura	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
12.2	Estabelecer e manter uma arquitetura de rede segura	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
12.2	Estabelecer e manter uma arquitetura de rede segura	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.
12.3	Gerenciar com segurança a infraestr utura de rede	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
13.1	Centralizar os alertas de eventos de segurança	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.1	Centralizar os alertas de eventos de segurança	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.3	Implementar uma solução de detecção de intrusões na rede	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.6	Coletar logs de fluxo de tráfego de rede	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.6	Coletar logs de fluxo de tráfego de rede	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-envvar-awscred-check	Certifique-se de que as credencia is de autentica ção AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptogra fado. Armazenar essas variáveis em texto não criptogra fado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para controles críticos de segurança do CIS v8 IG2.

Práticas recomendadas operacionais para CIS Critical Security Controls v8 IG3

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Center for Internet Security (CIS) Critical Security Controls v8 IG3 e as regras gerenciadas do AWS Config. Cada um AWS Config se aplica a um AWS recurso específico e está relacionado a um ou mais controles CIS Critical Security Controls v8 IG3. Um controle do CIS Critical Security Controls v8 IG3 pode estar relacionado a várias regras do AWS Config . Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			que o permitido pelos padrões da organizaç ão.
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.1	Estabelecer e manter um inventário detalhado dos ativos corporativos	ec2-security-group-attached-to-eni	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
2.2	Verificar se o software autorizado tem suporte atualmente	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Verificar se o software autorizado tem suporte atualmente	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrad o um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataform a. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataform a.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Utilizar ferramentas automatizadas de inventário de software	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Utilizar ferramentas automatizadas de inventário de software	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
3.3	Configurar listas de controle de acesso a dados	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.3	Configurar listas de controle de acesso a dados	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
3.3	Configurar listas de controle de acesso a dados	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.3	Configurar listas de controle de acesso a dados	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.3	Configurar listas de controle de acesso a dados	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3	Configurar listas de controle de acesso a dados	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.3	Configurar listas de controle de acesso a dados	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).
3.3	Configurar listas de controle de acesso a dados	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Configurar listas de controle de acesso a dados	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
3.4	Aplicar a retenção de dados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Aplicar a retenção de dados	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
3.10	Criptografar dados confidenciais em trânsito	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.10	Criptografar dados confidenciais em trânsito	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.10	Criptografar dados confidenciais em trânsito	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.10	Criptografar dados confidenciais em trânsito	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
3.11	Criptografar dados confidenciais em repouso	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
3.11	Criptografar dados confidenciais em repouso	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11	Criptografar dados confidenciais em repouso	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
3.11	Criptografar dados confidenciais em repouso	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
3,14	Acessar log de dados confidenciais	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
3,14	Acessar log de dados confidenciais	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3,14	Acessar log de dados confidenciais	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
4.1	Estabelecer e manter um processo de configuração seguro	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.
4.1	Estabelecer e manter um processo de configuração seguro	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Estabelecer e manter um processo de configuração seguro	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporati vos com segurança	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporati vos com segurança	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporati vos com segurança	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
4.6	Gerenciar ativos e softwares corporati vos com segurança	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.6	Gerenciar ativos e softwares corporativos com segurança	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4.6	Gerenciar ativos e softwares corporativos com segurança	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.7	Gerenciar contas padrão em ativos e software corporativos	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
5.1	Estabelecer e manter um inventário de contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Usar senhas exclusivas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.3	Desabilitar contas inativas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Restringir os privilégios de administrador às contas de administrador dedicadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6	Centralizar o gerenciamento de contas	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.4	Exigir MFA para acesso remoto à rede	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.5	Exigir MFA para acesso administrativo	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.7	Centralizar o controle de acesso	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1	Estabelecer e manter um processo de gerenciamento de vulnerabilidades	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.3	Executar o gerenciamento automatizado de patches do sistema operacional	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.4	Executar o gerenciamento automatizado de patches de aplicações	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7,5	Executar verificações automatizadas de vulnerabilidades de ativos corporativos internos	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.
8.1	Estabelecer e manter um processo de gerenciamento de logs de auditoria	audit-log-policy-exists (Verificação do processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
8.2	Coletar logs de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
8.2	Coletar logs de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2	Coletar logs de auditoria	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
8.3	Garantir o armazenamento adequado dos logs de auditoria	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
8.5	Coletar logs de auditoria detalhados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
8.5	Coletar logs de auditoria detalhados	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.5	Coletar logs de auditoria detalhados	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.7	Coletar logs de auditoria de solicitaç ões de URL	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.
8.9	Centralizar os logs de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.10	Reter logs de auditoria	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
8.10	Reter logs de auditoria	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implantar e manter um software antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2	Configurar atualizações automáticas de assinatura antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.4	Configurar a verificação antimalware automática de mídia removível	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.6	Gerenciar centralmente o software antimalware	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.7	Usar um software antimalware baseado em comportamento	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.2	Fazer backups automatizados	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	Fazer backups automatizados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
11.3	Proteger os dados de recuperação	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
11.3	Proteger os dados de recuperação	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Proteger os dados de recuperação	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Estabelecer e manter uma instância isolada de dados de recuperação	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
12.2	Estabelecer e manter uma arquitetura de rede segura	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
12.2	Estabelecer e manter uma arquitetura de rede segura	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
12.2	Estabelecer e manter uma arquitetura de rede segura	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
12.2	Estabelecer e manter uma arquitetura de rede segura	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
12.2	Estabelecer e manter uma arquitetura de rede segura	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
12.2	Estabelecer e manter uma arquitetura de rede segura	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.2	Estabelecer e manter uma arquitetura de rede segura	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.
12.3	Gerenciar com segurança a infraestr utura de rede	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.3	Gerenciar com segurança a infraestrutura de rede	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3	Gerenciar com segurança a infraestrutura de rede	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.6	Usar protocolos seguros de gerenciamento e comunicação de rede	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
13.1	Centralizar os alertas de eventos de segurança	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.1	Centralizar os alertas de eventos de segurança	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.3	Implementar uma solução de detecção de intrusões na rede	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.6	Coletar logs de fluxo de tráfego de rede	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.6	Coletar logs de fluxo de tráfego de rede	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13.10	Executar a filtragem da camada da aplicação	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-envvar-awscred-check	Certifique-se de que as credencia is de autentica ção AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptogra fado. Armazenar essas variáveis em texto não criptogra fado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do privilégio mínimo, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.1	Estabelecer e manter um processo seguro de desenvolvimento de aplicações	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.12	Implementar verificações de segurança no nível do código	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.12	Implementar verificações de segurança no nível do código	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.12	Implementar verificações de segurança no nível do código	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do privilégio mínimo, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.
16.12	Implementar verificações de segurança no nível do código	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16.12	Implementar verificações de segurança no nível do código	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para controles críticos de segurança do CIS v8 IG3.

Práticas recomendadas operacionais para o CIS Top 20

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre os 20 principais controles de segurança críticos do Center for Internet Security (CIS) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do CIS Top 20. Um controle do CIS Top 20 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse pacote de conformidade foi validado pela AWS Security Assurance Services LLC (AWS SAS), que é uma equipe de avaliadores de segurança qualificados do setor de cartões de pagamento (QSAs), profissionais certificados pela HITRUST Common Security Framework (CCSFPs) e profissionais de conformidade certificados para fornecer orientação e avaliações para várias estruturas do setor. AWS Os profissionais do SAS criaram esse Pacote de Conformidade para permitir que um cliente se alinhe a um subconjunto do CIS Top 20.

ID de controle	AWS Config Regra	Orientação
CIS.2	ec2- -check managedinstance-association-compliance-status	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.
CIS.2	ec2- -check managedinstance-patch-compliance-status	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2

ID de controle	AWS Config Regra	Orientação
		estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedime ntos da sua organização.
CIS.2	ec2- security-group-attached- to -eni	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
CIS.2	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2), verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	AWS Config Regra	Orientação
CIS.2	ec2- volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
CIS.2	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Config Regra	Orientação
CIS.3	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.3	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Config Regra	Orientação
CIS.3	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
CIS.4	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Config Regra	Orientação
CIS.4	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
CIS.4	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Config Regra	Orientação
CIS.4	root-account-hardware-mfa-habilitado	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
CIS.4	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Config Regra	Orientação
CIS.4	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
CIS.5	ec2- -manager instance-managed-by-systems	É possível fazer um inventári o das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacion al, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	AWS Config Regra	Orientação
CIS.5	ec2- -check managedinstance-association-compliance-status	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.
CIS.5	ec2- -check managedinstance-patch-compliance-status	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Config Regra	Orientação
CIS.5	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.5	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
CIS.6	api-gw-execution-logging-habilitado	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	AWS Config Regra	Orientação
CIS.6	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CIS.6	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Config Regra	Orientação
CIS.6	cloud-trail-log-file-habilitado para validação	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
CIS.6	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da Conta da AWS que acessou um bucket, endereço IP e horário do evento do Amazon S3.

ID de controle	AWS Config Regra	Orientação
CIS.6	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
CIS.6	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Config Regra	Orientação
CIS.6	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.6	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Config Regra	Orientação
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todos Regiões da AWS para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Config Regra	Orientação
CIS.6	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.6	s3- bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Config Regra	Orientação
CIS.6	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
CIS.6	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Config Regra	Orientação
CIS.8	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.9	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
CIS.9	ebs-snapshot-public-restora ble-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.9	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CIS.9	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Config Regra	Orientação
CIS.9	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
CIS.9	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Config Regra	Orientação
CIS.9	ec2- instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Config Regra	Orientação
CIS.9	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CIS.9	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Config Regra	Orientação
CIS.9	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Config Regra	Orientação
CIS.9	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.9	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.9	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.9	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.9	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
CIS.9	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Config Regra	Orientação
CIS.9	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CIS.9	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CIS.9	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Config Regra	Orientação
CIS.9	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
CIS.10	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.

ID de controle	AWS Config Regra	Orientação
CIS.10	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CIS.10	elasticache-redis-cluster-automatic-verificação de backup	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Config Regra	Orientação
CIS.10	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
CIS.10	s3- bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Config Regra	Orientação
CIS.11	ec2- security-group-attached-to -eni	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
CIS.11	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Config Regra	Orientação
CIS.11	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
CIS.11	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Config Regra	Orientação
CIS.11	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
CIS.12	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.12	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CIS.12	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.12	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
CIS.12	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.12	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.12	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Config Regra	Orientação
CIS.12	ec2- instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Config Regra	Orientação
CIS.12	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CIS.12	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Config Regra	Orientação
CIS.12	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Config Regra	Orientação
CIS.12	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.12	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.12	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.12	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.12	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
CIS.12	s3- bucket-public-read-prohibit ed	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Config Regra	Orientação
CIS.12	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CIS.12	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Config Regra	Orientação
CIS.12	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
CIS.12	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Config Regra	Orientação
CIS.12	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
CIS.13	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.13	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CIS.13	api-gw-cache-enablede criptografado	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
CIS.13	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Config Regra	Orientação
CIS.13	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
CIS.13	ec2- ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CIS.13	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
CIS.13	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	AWS Config Regra	Orientação
CIS.13	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
CIS.13	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
CIS.13	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Config Regra	Orientação
CIS.13	kms-cmk-not-scheduled-para exclusão	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
CIS.13	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.13	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
CIS.13	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.13	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CIS.13	s3- bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
CIS.13	habilitado para s3 bucket-server-side-encryption	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.13	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CIS.13	sagemaker-endpoint-configuration-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Config Regra	Orientação
CIS.13	sagemaker-notebook-instance-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.
CIS.13	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.14	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
CIS.14	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CIS.14	api-gw-cache-enablede criptografado	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.14	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
CIS.14	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
CIS.14	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
CIS.14	ebs-snapshot-public-restora ble-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.14	ec2- ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
CIS.14	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CIS.14	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	AWS Config Regra	Orientação
CIS.14	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
CIS.14	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Config Regra	Orientação
CIS.14	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.
CIS.14	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Config Regra	Orientação
CIS.14	kms-cmk-not-scheduled-para exclusão	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
CIS.14	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Config Regra	Orientação
CIS.14	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
CIS.14	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.14	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.14	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
CIS.14	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.14	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePub licAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPubl icAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
CIS.14	s3- bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.14	s3- bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
CIS.14	s3- bucket-public-read-prohibit ed	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CIS.14	s3- bucket-public-write-prohibi ted	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Config Regra	Orientação
CIS.14	habilitado para s3 bucket-server-side-encryption	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
CIS.14	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CIS.14	sagemaker-endpoint-configuration-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Config Regra	Orientação
CIS.14	sagemaker-notebook-instance-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.
CIS.14	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Config Regra	Orientação
CIS.16	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.16	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
CIS.16	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Config Regra	Orientação
CIS.16	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Config Regra	Orientação
CIS.16	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.16	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Config Regra	Orientação
CIS.16	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUp percaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básic as: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo

ID de controle	AWS Config Regra	Orientação
		rdAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
CIS.16	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Config Regra	Orientação
CIS.16	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
CIS.16	iam-user-group-membership-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Config Regra	Orientação
CIS.16	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.
CIS.16	iam-user-no-policies-verificar	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Config Regra	Orientação
CIS.16	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Config Regra	Orientação
CIS.16	mfa-enabled-for-iam-acesso ao console	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
CIS.16	root-account-hardware-mfa-h abilitado	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Config Regra	Orientação
CIS.16	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
CIS.16	secretsmanager-rotation-ena bled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programaç ão regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	AWS Config Regra	Orientação
CIS.16	secretsmanager-scheduled-rotation-success-verificar	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
CIS.16	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Config Regra	Orientação
CIS.18	codebuild-project-envvar-awscred-verificar	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.
CIS.18	codebuild-project-source-repo-verificação de URL	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	AWS Config Regra	Orientação
CIS.19	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
CIS.19	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Config Regra	Orientação
CIS.19	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
CIS.2	ec2- -manager instance-managed-by-systems	É possível fazer um inventári o das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacion al, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o CIS Top 20.

Prática recomendadas operacionais para o CISA Cyber Essentials

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Cybersecurity & Infrastructure Security Agency (CISA), o Cyber Essentials (CE) e as regras gerenciadas do AWS Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles CISA CE. Um controle CISA CE pode estar relacionado a várias AWS Config regras. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Staff-1	Desenvolva uma cultura de conscientização para incentivar os funcionários a fazerem boas escolhas on-line.	security-awareness-program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Staff-2	Saiba mais sobre riscos como phishing e comprometimento do e-mail corporati vo.XXXXX.	security-awareness -program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
Your Staff-3	Preste atenção aos eventos atuais relacionados à segurança cibernéti ca, usando as lições aprendidas e os eventos relatados para permanece r alerta quanto ao ambiente de ameaças atual e ágil quanto às tendências de segurança cibernéti ca.	security-awareness -program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Staff-4	Use o treinamento básico em segurança cibernética para melhorar a exposição aos conceitos , terminologia e atividades de segurança cibernéti ca associados à implementação das práticas recomenda das de segurança cibernética.	security-awareness -program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
Your Staff-5	Identifique os recursos de treinamen to disponíveis por meio de associações profissionais, instituiç ões acadêmicas, setor privado e fontes governamentais.	security-awareness -program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-1	Conheça bem sua rede. Mantenha inventários de ativos de hardware e software para saber o que está em jogo e o que corre risco de ataque.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-2	Como utilizar atualizações automáticas para todos os sistemas operacionais e software de terceiros.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-2	Como utilizar atualizações automáticas para todos os sistemas operacionais e software de terceiros.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-2	Como utilizar atualizações automáticas para todos os sistemas operacionais e software de terceiros.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-2	Como utilizar atualizações automáticas para todos os sistemas operacionais e software de terceiros.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas depois de atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	opensearch-data-node-fault-tolerance	O Amazon OpenSearch Service (OpenSearch Service) exige pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um domínio OpenSearch de serviço com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	secretsmanager-secret-periodic-rotation	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação periódica ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido. O valor padrão é 90 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-3	Implemente configurações de segurança para todos os ativos de hardware e software.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Systems-4	Remova hardware e software não suportados ou não autorizados dos sistemas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-1	Conheça bem quem usa sua rede. Mantenha inventários de conexões de rede (usuários, fornecedores, parceiros de negócios etc.).	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
Your Surroundings-1	Conheça bem quem usa sua rede. Mantenha inventários de conexões de rede (usuários, fornecedores, parceiros de negócios etc.).	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-1	Conheça bem quem usa sua rede. Mantenha inventários de conexões de rede (usuários, fornecedores, parceiros de negócios etc.).	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Your Surroundings-2	Aproveite a autenticação multifatorial para todos os usuários, começando com usuários privilegiados, administrativos e de acesso remoto.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-2	Aproveite a autentica ção multifatorial para todos os usuários, começando com usuários privilegiados, administrativos e de acesso remoto.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-2	Aproveite a autenticação multifatorial para todos os usuários, começando com usuários privilegiados, administrativos e de acesso remoto.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-2	Aproveite a autenticação multifatorial para todos os usuários, começando com usuários privilegiados, administrativos e de acesso remoto.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Conceda permissões de acesso e de administrador com base no need-to-know menor privilégio.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Surroundings-3	Use senhas exclusivas para cada um dos usuários.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
Your Data-1	Saiba como seus dados são protegidos.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
Your Data-1	Saiba como seus dados são protegidos.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-1	Saiba como seus dados são protegidos.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Your Data-1	Saiba como seus dados são protegidos.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
Your Data-1	Saiba como seus dados são protegidos.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
Your Data-1	Saiba como seus dados são protegidos.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
Your Data-1	Saiba como seus dados são protegidos.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-1	Saiba como seus dados são protegidos.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-1	Saiba como seus dados são protegidos.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-1	Saiba como seus dados são protegidos.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-1	Saiba como seus dados são protegidos.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
Your Data-1	Saiba como seus dados são protegidos.	backup-recovery-po int-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	opensearch-node-to -node-encryption-c heck	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	sagemaker-endpoint -configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	backup-recovery-po int-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro , componentes do host e do dispositi vo e atividades em trânsito data-at-rest e de comportamento do usuário.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-2	Saiba o que está acontecendo na sua rede. Gerencie componentes de rede e perímetro, componentes do host e do dispositivo e atividades em trânsito data-at-rest e de comportamento do usuário.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-3	Proteção do sistema de nomes de domínio.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-4	Estabeleça backups e redundâncias automatizados regulares dos principais sistemas.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Data-5	Aproveite as proteções para backups, incluindo segurança física, criptografia e cópias off-line.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
Your Data-5	Aproveite as proteções para backups, incluindo segurança física, criptografia e cópias off-line.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Crisis Response-2	Liderar o desenvolvimento de uma estrutura interna de relatórios para detectar, comunicar e conter ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Your Crisis Response-2	Liderar o desenvolvimento de uma estrutura interna de relatórios para detectar, comunicar e conter ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	ebs-optimized-inst ance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimizaçã o proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configurações do sistema.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configura ções do sistema.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configurações do sistema.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (1)	Empregue uma solução de backup que funcione de maneira automática e contínua de dados críticos e configurações do sistema.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (2)	Exija a autentica ção multifator (MFA) para acessar seus sistemas sempre que possível. A MFA deve ser exigida de todos os usuários, mas comece com usuários privilegiados, administrativos e de acesso remoto.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (2)	Exija a autentica ção multifator (MFA) para acessar seus sistemas sempre que possível. A MFA deve ser exigida de todos os usuários, mas comece com usuários privilegiados, administrativos e de acesso remoto.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (2)	Exija a autentica ção multifator (MFA) para acessar seus sistemas sempre que possível. A MFA deve ser exigida de todos os usuários, mas comece com usuários privilegiados, administrativos e de acesso remoto.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (2)	Exija a autentica ção multifator (MFA) para acessar seus sistemas sempre que possível. A MFA deve ser exigida de todos os usuários, mas comece com usuários privilegiados, administrativos e de acesso remoto.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (3)	Habilite as atualizações automáticas sempre que possível. Substitua sistemas operacionais, aplicações e hardware não compatíveis. Teste e implante patches rapidamente.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (3)	Habilite as atualizações automáticas sempre que possível. Substitua sistemas operacionais, aplicações e hardware não compatíveis. Teste e implante patches rapidamente.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (3)	Habilite as atualizações automáticas sempre que possível. Substitua sistemas operacionais, aplicações e hardware não compatíveis. Teste e implante patches rapidamente.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Inicialização: o que fazer primeiro (3)	Habilite as atualizações automáticas sempre que possível. Substitua sistemas operacionais, aplicações e hardware não compatíveis. Teste e implante patches rapidamente.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o CISA Cyber Essentials.

Práticas recomendadas operacionais para Serviços de Informação da Justiça Criminal (CJIS)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os requisitos de conformidade dos Serviços de Informações da Justiça Criminal (CJIS) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CJIS. Um controle do CJIS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.2	Treinamento de conscientização sobre segurança	security-awareness -program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ou incidentes de segurança.
5.3	Resposta a incidentes	response-plan-exists-maintained (Verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.
5.3	Resposta a incidentes	response-plan-tested (Verificação do processo)	Teste os planos de recuperação e resposta a incidentes. Isso pode ajudar a saber se o plano será eficaz durante um incidente e se alguma lacuna ou atualização precisa ser resolvida.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4	Auditoria e responsabilidade	audit-log-policy-exists (Verificação do processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
5.4.1	Eventos e conteúdos auditáveis (sistemas de informação)	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.5	Proteção de informações de auditoria	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.5	Proteção de informações de auditoria	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.5	Proteção de informações de auditoria	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.
5.4.6	Retenção de registros de auditoria	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.4.6	Retenção de registros de auditoria	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
5.5.2	Fiscalização de acesso	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor de CJIS: falso), RequireLowercaseCharacters (valor de CJIS: falso), RequireSymbols (valor de CJIS: falso), (valor de CJIS: falso), RequireNumbers (valor de CJIS: 8), MinimumPasswordLength (valor de CJIS: 10) e PasswordReusePrevention MaxPasswo

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			rdAge (valor de CJIS: 90) para sua política de senha do IAM. Os valores reais devem refletir as políticas da organização.
5.5.2	Fiscalização de acesso	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, pois a autenticação é gerenciada externamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2	Fiscalização de acesso	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner™.
5.5.2.1	Privilégio mínimo	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
5.5.2.1	Privilégio mínimo	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
5.5.2.1	Privilégio mínimo	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	ecs-containers-non privileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner™ não pode ser modificado a menos que tenha permissões explícitas de leitura e gravação.
5.5.2.1	Privilégio mínimo	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.2.1	Privilégio mínimo	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.6	Acesso remoto	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.5.6	Acesso remoto	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.2.1.1	Senha	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor de CJIS: falso), RequireLowercaseCharacters (valor de CJIS: falso), RequireSymbols (valor de CJIS: falso), (valor de CJIS: falso), RequireNumbers (valor de CJIS: 8), MinimumPasswordLength (valor de CJIS: 10) e PasswordReusePrevention MaxPasswo

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			rdAge (valor de CJIS: 90) para sua política de senha do IAM. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.2.2	Autenticação avançada	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
5.6.2.2	Autenticação avançada	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.2.2	Autenticação avançada	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.2.2	Autenticação avançada	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.2.2	Autenticação avançada	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.6.3.1	Gerenciamento de identificadores	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
5.7.1.1	Funcionalidade mínima	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
5.7.1.1	Funcionalidade mínima	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
5.7.1.1	Funcionalidade mínima	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
5.7.1.1	Funcionalidade mínima	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
5.7.1.1	Funcionalidade mínima	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
5.7.1.1	Funcionalidade mínima	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
5.7.1.1	Funcionalidade mínima	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
5.7.1.1	Funcionalidade mínima	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.7.1.1	Funcionalidade mínima	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.
5.10	Proteção de sistemas e comunicações e integridade das informações	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10	Proteção de sistemas e comunicações e integridade das informações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10	Proteção de sistemas e comunicações e integridade das informações	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
5.10	Proteção de sistemas e comunicações e integridade das informações	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
5.10.1	Fiscalização de fluxo de informações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1	Fiscalização de fluxo de informações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
5.10.1	Fiscalização de fluxo de informações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
5.10.1	Fiscalização de fluxo de informações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
5.10.1	Fiscalização de fluxo de informações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
5.10.1	Fiscalização de fluxo de informações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
5.10.1	Fiscalização de fluxo de informações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
5.10.1	Fiscalização de fluxo de informações	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1	Fiscalização de fluxo de informações	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1.1	Proteção de limites	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
5.10.1.1	Proteção de limites	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
5.10.1.1	Proteção de limites	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
5.10.1.1	Proteção de limites	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.1	Proteção de limites	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
5.10.1.2	Criptografia	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1.2	Criptografia	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
5.10.1.2	Criptografia	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
5.10.1.2	Criptografia	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
5.10.1.2	Criptografia	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenad os no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
5.10.1.2	Criptografia	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
5.10.1.2	Criptografia	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
5.10.1.2	Criptografia	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1.2	Criptografia	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
5.10.1.2	Criptografia	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
5.10.1.2	Criptografia	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1.2	Criptografia	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
5.10.1.2	Criptografia	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
5.10.1.2	Criptografia	backup-recovery-po int-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
5.10.1.2	Criptografia	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.2	Criptografia	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.3	Ferramentas e técnicas de detecção de intrusões	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.3	Ferramentas e técnicas de detecção de intrusões	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.1.3	Ferramentas e técnicas de detecção de intrusões	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.1	Gerenciamento de patches	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.1	Gerenciamento de patches	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.1	Gerenciamento de patches	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.1	Gerenciamento de patches	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.1	Gerenciamento de patches	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.4	Alertas e recomendações de segurança	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.4	Alertas e recomendações de segurança	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5.10.4.4	Alertas e recomendações de segurança	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CJIS.

Práticas recomendadas operacionais para a CMMC Nível 1

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) Nível 1 e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC de nível 1. Um controle da CMMC Nível 1 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restaurável eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantind o que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.211	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC de nível 1.

Práticas recomendadas operacionais para a CMMC Nível 2

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) Nível 2 e as regras gerenciadas AWS do Config. Cada regra de Config se

aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC de nível 2. Um controle da CMMC Nível 2 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC.2.013	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.2.159	Desenvolva e implemente planos de ação criados para corrigir deficiências e reduzir ou eliminar vulnerabilidades nos sistemas organizac ionais.	vuln-management-pl an-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferrament as de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alteraçõe s nos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.078	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.079	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	response-plan-exists-maintained (Verifica ção do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuí dos à equipe responsável. Ter planos de resposta formalmente atualizad os e documenta dos pode ajudar a garantir que a equipe de resposta compreenda as funções, responsab ilidades e processos a serem seguidos durante um incidente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
IR.2.093	Detecte e relate eventos.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autenticação multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutenção não local for concluída.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.2.137	Execute e teste regularmente backups de dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	vuln-scans-performed (Verificação do processo)	Garanta que as verificações de vulnerabilidade sejam realizadas de acordo com seus requisitos de conformidade. A frequência da verificação, as ferramentas usadas e o uso dos resultados devem ser definidos pela sua organização.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.211	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC de nível 2.

Práticas recomendadas operacionais para a CMMC Nível 3

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) Nível 3 e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC de nível 3. Um controle da CMMC Nível 3 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

> **Note**
>
> Devido à orientação provisória fornecida pelo DoD e pelo Organismo de Credenciamento do CMMC com relação à reciprocidade do FedRAMP para CMMC de nível 3 a 5, é recomendável que os clientes AWS GovCloud usem as regiões (EUA) atualmente para qualquer carga de trabalho que exija conformidade com o CMMC de nível 3 a 5. Dessa forma, os modelos de pacotes de conformidade para a CMMC Níveis 3-5 não estão disponíveis no console do pacote de conformidade para evitar confusão. Os clientes podem instalar de forma independente as regras do Config que mapeiam a orientação provisória para o CMMC de nível 3-5 (sem um modelo de pacote de conformidade) CloudFormation usando o arquivo YAML de amostra vinculado a este documento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restaurávveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC.2.013	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.2.159	Desenvolva e implemente planos de ação criados para corrigir deficiências e reduzir ou eliminar vulnerabilidades nos sistemas organizac ionais.	vuln-management-pl an-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferrament as de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.078	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.079	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
IR.2.093	Detecte e relate eventos.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.2.137	Execute e teste regularmente backups de dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.211	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.213	Faça verificações periódicas do sistema de informações e verificações em tempo real de arquivos de origens externas à medida que os arquivos são baixados, abertos ou executados.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC de nível 3.

Práticas recomendadas operacionais para a CMMC Nível 4

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) Nível 4 e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC de nível 4. Um controle da CMMC Nível 4 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

> **Note**
>
> Devido à orientação provisória fornecida pelo DoD e pelo Organismo de Credenciamento do CMMC com relação à reciprocidade do FedRAMP para CMMC de nível 3 a 5, é recomendável que os clientes AWS GovCloud usem as regiões (EUA) atualmente para qualquer carga de trabalho que exija conformidade com o CMMC de nível 3 a 5. Dessa forma, os modelos de pacotes de conformidade para a CMMC Níveis 3-5 não estão disponíveis no console do pacote de conformidade para evitar confusão. Os clientes podem instalar de forma independente as regras do Config que mapeiam a orientação provisória para o CMMC de nível 3-5 (sem um modelo de pacote de conformidade) CloudFormation usando o arquivo YAML de amostra vinculado a este documento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC.2.013	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividade s suspeitas definidas pela organização.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informaçõ es de auditoria para atividades amplas, além da atividade por máquina.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informações de auditoria para atividades amplas, além da atividade por máquina.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informaçõ es de auditoria para atividades amplas, além da atividade por máquina.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.078	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.079	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegiadas.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
IR.2.093	Detecte e relate eventos.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autenticação multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutenção não local for concluída.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.2.137	Execute e teste regularmente backups de dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.150	Use a inteligência contra ameaças para informar o desenvolvimento do sistema e das arquiteturas de segurança, seleção de soluções de segurança, monitoramento, busca de ameaças e atividades de resposta e recuperação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA.4.171	Estabeleça e mantenha uma capacidade de busca de ameaças cibernéticas para procurar indicador es de compromet imento em sistemas organizacionais e detectar, rastrear e interromper ameaças que escapam aos controles existentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SC.1.175	Monitore, controle e proteja as comunicaç ões organizac ionais (ou seja, informações transmiti das ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.199	Utilize inteligência contra ameaças para impedir proativam ente que solicitações de DNS cheguem a domínios maliciosos.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.199	Utilize inteligência contra ameaças para impedir proativam ente que solicitações de DNS cheguem a domínios maliciosos.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.202	Empregue mecanismos para analisar códigos e scripts executáveis (por exemplo, sandbox) atravessando os limites da rede da Internet ou outros limites definidos pela organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.211	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.213	Faça verificações periódicas do sistema de informações e verificações em tempo real de arquivos de origens externas à medida que os arquivos são baixados, abertos ou executados.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.4.221	Use informações de indicadores de ameaças relevantes para as informações e sistemas que estão sendo protegidos e mitigações eficazes obtidas de organizações externas para informar a detecção de invasões e a busca de ameaças.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC de nível 4.

Práticas recomendadas operacionais para a CMMC Nível 5

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) Nível 5 e as regras gerenciadas AWS do Config. Cada regra de Config se

aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC de nível 5. Um controle da CMMC Nível 5 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

> **Note**
>
> Devido à orientação provisória fornecida pelo DoD e pelo Organismo de Credenciamento do CMMC com relação à reciprocidade do FedRAMP para CMMC de nível 3 a 5, é recomendável que os clientes AWS GovCloud usem as regiões (EUA) atualmente para qualquer carga de trabalho que exija conformidade com o CMMC de nível 3 a 5. Dessa forma, os modelos de pacotes de conformidade para a CMMC Níveis 3-5 não estão disponíveis no console do pacote de conformidade para evitar confusão. Os clientes podem instalar de forma independente as regras do Config que mapeiam a orientação provisória para o CMMC de nível 3-5 (sem um modelo de pacote de conformidade) CloudFormation usando o arquivo YAML de amostra vinculado a este documento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restaurávveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.001	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.002	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.1.003	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.007	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.008	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC.2.013	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.013	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.2.016	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.3.014	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.017	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.3.018	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.4.023	Controle os fluxos de informações entre domínios de segurança em sistemas conectados.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.5.024	Identifique e mitigue riscos associados a pontos de acesso sem fio não identificados conectados à rede.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AM.4.226	Empregue a capacidade de descobrir e identificar sistemas com atributos de componentes específicos (por exemplo, nível de firmware, tipo de sistema operacional) em seu inventário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.041	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.2.042	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.046	Alerta em caso de falha no processo de registro em log de uma auditoria.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.049	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.3.051	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividade s suspeitas definidas pela organização.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.053	Automatize a análise de logs de auditoria para identificar e agir em relação a indicadores críticos (TTPs) e/ou atividades suspeitas definidas pela organização.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informaçõ es de auditoria para atividades amplas, além da atividade por máquina.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informaçõ es de auditoria para atividades amplas, além da atividade por máquina.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.4.054	Analise as informações de auditoria para atividades amplas, além da atividade por máquina.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriad os definidos pela organização estejam registrando.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriad os definidos pela organização estejam registrando.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.5.055	Identifique os ativos que não relatam registros de auditoria e garanta que os sistemas apropriados definidos pela organização estejam registrando.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.3.161	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.061	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.062	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.063	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.064	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.2.065	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.3.068	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.5.074	Verifique a integrida de e a exatidão do software essencial ou essencial de segurança, conforme definido pela organização (por exemplo, raízes de confiança, verificação formal ou assinaturas criptográficas).	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.5.074	Verifique a integrida de e a exatidão do software essencial ou essencial de segurança, conforme definido pela organização (por exemplo, raízes de confiança, verificação formal ou assinaturas criptográficas).	ec2-instance-manag ed-by-systems-mana ger	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.5.074	Verifique a integrida de e a exatidão do software essencial ou essencial de segurança, conforme definido pela organização (por exemplo, raízes de confiança, verificação formal ou assinaturas criptográficas).	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.5.074	Verifique a integrida de e a exatidão do software essencial ou essencial de segurança, conforme definido pela organização (por exemplo, raízes de confiança, verificação formal ou assinaturas criptográficas).	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.076	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.1.077	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.078	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.079	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.2.081	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.083	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.3.086	Desabilite os identificadores após um período definido de inatividade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.092	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
IR.2.093	Detecte e relate eventos.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.2.093	Detecte e relate eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.5.102	Use uma combinação de respostas manuais e automatizadas em tempo real para atividades anômalas que correspondam aos padrões de incidentes.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.5.102	Use uma combinação de respostas manuais e automatizadas em tempo real para atividades anômalas que correspondam aos padrões de incidentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.5.102	Use uma combinação de respostas manuais e automatizadas em tempo real para atividades anômalas que correspondam aos padrões de incidentes.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.5.102	Use uma combinação de respostas manuais e automatizadas em tempo real para atividades anômalas que correspondam aos padrões de incidentes.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.2.113	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.2.137	Execute e teste regularmente backups de dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.137	Execute e teste regularmente backups de dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.2.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.3.139	Execute regularmente backups de dados completos, abrangentes e resilientes, conforme definido pela organização.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RE.5.140	Garanta que as instalações de processamento de informações atendam aos requisitos de continuidade, redundância e disponibilidade de segurança da informação definidos pela organização.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.2.142	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.150	Use a inteligência contra ameaças para informar o desenvolvimento do sistema e das arquiteturas de segurança, seleção de soluções de segurança, monitoramento, busca de ameaças e atividades de resposta e recuperação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RM.4.151	Execute verificações de portas não autorizadas disponíveis nos limites da rede perimetral, nos limites da rede de Internet da organização e em outros limites definidos pela organização.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA.4.171	Estabeleça e mantenha uma capacidade de busca de ameaças cibernéticas para procurar indicador es de compromet imento em sistemas organizacionais e detectar, rastrear e interromper ameaças que escapam aos controles existentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SC.1.175	Monitore, controle e proteja as comunicaç ões organizac ionais (ou seja, informações transmiti das ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.1.175	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.2.179	Use sessões criptografadas para o gerenciamento de dispositivos de rede.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.180	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.182	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.185	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
SC.3.187	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.190	Proteja a autenticidade das sessões de comunicação.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.3.190	Proteja a autenticidade das sessões de comunicação.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC.3.191	Proteja a confidencialidade de CUI em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidencialidade de CUI em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC.3.191	Proteja a confidencialidade de CUI em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.3.191	Proteja a confidenc ialidade de CUI em repouso.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.199	Utilize inteligência contra ameaças para impedir proativam ente que solicitações de DNS cheguem a domínios maliciosos.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.199	Utilize inteligência contra ameaças para impedir proativam ente que solicitações de DNS cheguem a domínios maliciosos.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.4.202	Empregue mecanismos para analisar códigos e scripts executáve is (por exemplo, sandbox) atravessa ndo os limites da rede da Internet ou outros limites definidos pela organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.198	Configure sistemas de monitoramento para registrar pacotes que passam pelos limites da rede de Internet da organização e outros limites definidos pela organização.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.198	Configure sistemas de monitoramento para registrar pacotes que passam pelos limites da rede de Internet da organização e outros limites definidos pela organização.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.198	Configure sistemas de monitoramento para registrar pacotes que passam pelos limites da rede de Internet da organização e outros limites definidos pela organização.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.208	Use proteções de limites definidas e personalizadas na organização, além de soluções disponíveis comercialmente.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.5.230	Aplique a conformidade de portas e protocolos.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.5.230	Aplique a conformidade de portas e protocolos.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.5.230	Aplique a conformidade de portas e protocolos.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.5.230	Aplique a conformidade de portas e protocolos.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.210	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.211	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.1.213	Faça verificações periódicas do sistema de informações e verificações em tempo real de arquivos de origens externas à medida que os arquivos são baixados, abertos ou executados.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.214	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.216	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.2.217	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.4.221	Use informações de indicadores de ameaças relevantes para as informações e sistemas que estão sendo protegidos e mitigações eficazes obtidas de organizações externas para informar a detecção de invasões e a busca de ameaças.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.222	Analise o comportamento do sistema para detectar e mitigar a execução de comandos e scripts normais do sistema que indicam ações maliciosas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.5.223	Monitore indivíduos e componentes do sistema continuam ente em busca de comportamento anômalo ou suspeito.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC nível 5.

Práticas recomendadas operacionais para o CMMC 2.0 Nível 1

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) 2.0 Nível 1 e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC 2.0 de nível 1. Um controle do CMMC 2.0 Nível 1 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restaurávveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.2	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.5	Faça verificações periódicas do sistema de informações e verificações em tempo real de arquivos de origens externas à medida que os arquivos são baixados, abertos ou executados.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC 2.0 Nível 1.

Práticas recomendadas operacionais para a CMMC 2.0 Nível 2

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre a Certificação do Modelo de Maturidade de Cibersegurança (CMMC) 2.0 Nível 2 e as regras gerenciadas AWS do Config. Cada regra de

Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CMMC 2.0 de nível 2. Um controle da CMMC 2.0 Nível 2 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluindo outros sistemas de informação).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	iam-user-unused-credentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.1	Limite o acesso ao sistema de informações a usuários autorizados, processos que atuam em nome de usuários autorizados ou dispositivos (incluind o outros sistemas de informação).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informaçõ es aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.2	Limite o acesso do sistema de informações aos tipos de transações e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L1-3.1.20	Verifique e controle/limite as conexões aos sistemas de informações externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e capture a execução dessas funções nos logs de auditoria.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.12	Monitore e controle as sessões de acesso remoto.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.12	Monitore e controle as sessões de acesso remoto.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC.L2-3.1.12	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.12	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC.L2-3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividade s ilegais ou não autorizadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.1	Crie e retenha registros e logs de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais ou não autorizadas do sistema.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.4	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.4	Alerta em caso de falha no processo de registro em log de uma auditoria.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU.L2-3.3.4	Alerta em caso de falha no processo de registro em log de uma auditoria.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.4	Alerta em caso de falha no processo de registro em log de uma auditoria.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.5	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.5	Correlacione os processos de revisão, análise e relato de registros de auditoria para investigação e resposta a indícios de atividades ilegais, não autorizadas, suspeitas ou incomuns.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS
AU.L2-3.3.8	Proteja as informaçõ es de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificaç ões e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU.L2-3.3.8	Proteja as informações de auditoria e as ferramentas de registro em log de auditoria contra acessos, modificações e exclusões não autorizados.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
CA.L2-3.12.2	Desenvolva e implemente planos de ação criados para corrigir deficiências e reduzir ou eliminar vulnerabilidades nos sistemas organizacionais.	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferramentas de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.L2-3.12.3	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.L2-3.12.3	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA.L2-3.12.3	Monitore os controles de segurança constantemente para garantir a eficácia contínua dos controles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
CM.L2-3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologi a da informação usados em sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.2	Estabeleça e aplique configurações de segurança para produtos de tecnologia da informação usados em sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alteraçõe s nos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.3	Acompanhe, revise, aprove ou reprove e registre as alterações nos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolos e serviços não essenciais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.7	Restrinja, desabilite ou impeça o uso de programas, funções, portas, protocolo s e serviços não essenciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.9	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.9	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM.L2-3.4.9	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositi vos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.1	Identifique usuários do sistema de informações, processos que agem em nome dos usuários ou dispositivos.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L1-3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas de informações organizacionais.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegiadas.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.6	Desabilite os identificadores após um período definido de inatividade.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.6	Desabilite os identificadores após um período definido de inatividade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.7	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.8	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA.L2-3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.L2-3.6.1	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.L2-3.6.1	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.L2-3.6.1	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR.L2-3.6.1	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS
IR.L2-3.6.3	Teste a capacidad e organizacional de resposta a incidentes.	response-plan-test ed (Verificação do processo)	Teste os planos de recuperação e resposta a incidente s. Isso pode ajudar a saber se o plano será eficaz durante um incidente e se alguma lacuna ou atualização precisa ser resolvida.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.L2-3.7.5	Exija autentica ção multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutençã o não local for concluída.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
MA.L2-3.7.5	Exija autenticação multifator para estabelecer sessões de manutenção não locais por meio de conexões de rede externas e encerrar essas conexões quando a manutenção não local for concluída.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA.L2-3.11.2	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA.L2-3.11.2	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA.L2-3.11.2	Verifique se há vulnerabilidades em sistemas e aplicações organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA.L2-3.11.2	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam esses sistemas e aplicações são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L1-3.13.1	Monitore, controle e proteja as comunicações organizacionais (ou seja, informações transmitidas ou recebidas pelos sistemas de informações organizacionais) nos limites externos e nos principais limites internos dos sistemas de informações.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.4	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L2-3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.10	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas depois de atingirem o final do período criptográfico.
SC.L2-3.13.10	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC.L2-3.13.15	Proteja a autenticidade das sessões de comunicação.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidencialidade de CUI em repouso.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC.L2-3.13.16	Proteja a confidenc ialidade de CUI em repouso.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.1	Identifique, relate e corrija informações e falhas do sistema de informações em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.2	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas de informações organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L1-3.14.5	Faça verificações periódicas do sistema de informações e verificações em tempo real de arquivos de origens externas à medida que os arquivos são baixados, abertos ou executados.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI.L2-3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para CMMC 2.0 Nível 2.

Práticas recomendadas operacionais para serviços de computação

Esse pacote de conformidade contém AWS Config regras baseadas nos Serviços de computação. Para obter mais informações, consulte Compute for any workload. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de computação.

Práticas recomendadas operacionais para a resiliência de dados

Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para resiliência de dados.

Práticas recomendadas operacionais para serviços de bancos de dados

Esse pacote de conformidade contém AWS Config regras baseadas nos Serviços de Bancos de Dados. Para obter mais informações, consulte Bancos de dados ativados AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de bancos de dados.

Práticas recomendadas operacionais para o data lakes e os serviços de análise

Esse pacote de conformidade contém AWS Config regras para Data Lakes e Analytics Services. Para obter mais informações, consulte Data Lakes and Analytics on AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de data lakes e análise.

Práticas recomendadas operacionais para o DevOps

Este pacote de conformidade contém AWS Config regras baseadas em. DevOps AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para DevOps.

Práticas recomendadas operacionais para o EC2

Esse pacote de conformidade contém AWS Config regras baseadas no EC2. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para EC2.

Práticas recomendadas operacionais para criptografia e gerenciamento de chaves

Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para criptografia e gerenciamento de chaves.

Práticas recomendadas operacionais do Guia de segurança cibernética da ENISA para PMEs

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos

usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o guia de cibersegurança da Agência da União Europeia para Segurança Cibernética (ENISA) para PMEs e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais guias de segurança cibernética da ENISA para controles de PMEs. Um guia de segurança cibernética da ENISA para controle de PMEs pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este modelo de pacote de conformidade de amostra contém mapeamentos para controles adaptados do guia de segurança cibernética da ENISA para PMEs. O guia de segurança cibernética da ENISA para PMEs está disponível em Guia de segurança cibernética para PMEs - 12 etapas para proteger sua empresa.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: PUBLIQUE POLÍTICAS DE SEGURANÇA CIBERNÉTICAS	É preciso criar regras claras e específicas para a segurança cibernéticas	security-awareness-program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	dynamodb-table-encrypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	elasticsearch-encrypted-at-rest	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os domínios do Amazon Elasticsearch Service (Amazon ES).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	efs-access-point-e nforce-user-identity	Para ajudar na implementação do princípio de privilégi o mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configura da no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenad os no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	elasticsearch-node-to-node-encryption-check	Certifique-se de que a node-to-node criptografia para o Amazon Elasticse arch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	iam-policy-no-stat ements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriados estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriadas em vigor.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1_DESENVOLVER UMA BOA CULTURA DE SEGURANÇA CIBERNÉTICA: LEMBRE-SE DA PROTEÇÃO DE DADOS	De acordo com o Regulamento Geral de Proteção de Dados da UE1, todas as PMEs que processam ou armazenam dados pessoais de residentes da UE/EEE precisam garantir que os controles de segurança apropriad os estejam em vigor para proteger esses dados. Isso inclui garantir que todos que trabalham em nome da PME tenham medidas de segurança apropriad as em vigor.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2_FORNEÇA TREINAMENTO ADEQUADO	Ofereça treinamentos regulares de conscientização sobre segurança cibernética a todos os funcionários para que eles possam reconhecer e lidar com as várias ameaças à segurança cibernética. Esses treinamentos devem ser adaptados para PMEs e focar em situações reais. Forneça treinamento especializado em segurança cibernética aos responsáveis pelo gerenciamento da segurança cibernética na empresa para que eles tenham as habilidades e competências necessárias no trabalho que desempenham.	security-awareness-program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4_DESENVOLVA UM PLANO DE RESPOSTA A INCIDENTES	Desenvolva um plano formal de resposta a incidentes com diretrizes, funções e responsabilidades claras documentadas para responder a todos os incidentes de segurança de maneira oportuna, profissional e apropriada. Para responder rapidamente às ameaças à segurança, pesquise ferramentas que ajudem a monitorar e criar alertas quando ocorrerem atividades suspeitas ou violações de segurança.	response-plan-exists-maintained (verificação de processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5_PROTEJA O ACESSO AOS SISTEMAS	Incentive todos a usarem um código secreto com pelo menos três palavras comuns aleatória s combinadas para facilitar a memorizaç ão e melhorar a segurança. Se você optar por uma senha comum: - Ela precisa ser longa, com caracteres minúsculo s e maiúsculos, possivelmente também números e caracteres especiais . - Evite elementos óbvios, como “senha”, sequências de letras ou números como “abc”, números como “123”. - Evite usar informações pessoais que sejam encontradas on-line. E, se você usa códigos ou senhas, não as reutilize em outro lugar. - Não os compartilhe com colegas. - Habilite a Autenticação	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Multifatorial. - Use um gerenciador de senhas exclusivo.		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5_PROTEJA O ACESSO AOS SISTEMAS	Incentive todos a usarem um código secreto com pelo menos três palavras comuns aleatória s combinadas para facilitar a memorizaç ão e melhorar a segurança. Se você optar por uma senha comum: - Ela precisa ser longa, com caracteres minúsculo s e maiúsculos, possivelmente também números e caracteres especiais . - Evite elementos óbvios, como “senha”, sequências de letras ou números como “abc”, números como “123”. - Evite usar informações pessoais que sejam encontradas on-line. E, se você usa códigos ou senhas, não as reutilize em outro lugar. - Não os compartilhe com colegas. - Habilite a Autenticação	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Multifatorial. - Use um gerenciador de senhas exclusivo.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5_PROTEJA O ACESSO AOS SISTEMAS	Incentive todos a usarem um código secreto com pelo menos três palavras comuns aleatória s combinadas para facilitar a memorizaç ão e melhorar a segurança. Se você optar por uma senha comum: - Ela precisa ser longa, com caracteres minúsculo s e maiúsculos, possivelmente também números e caracteres especiais . - Evite elementos óbvios, como “senha”, sequências de letras ou números como “abc”, números como “123”. - Evite usar informações pessoais que sejam encontradas on-line. E, se você usa códigos ou senhas, não as reutilize em outro lugar. - Não os compartilhe com colegas. - Habilite a Autenticação	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Multifatorial. - Use um gerenciador de senhas exclusivo.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5_PROTEJA O ACESSO AOS SISTEMAS	Incentive todos a usarem um código secreto com pelo menos três palavras comuns aleatória s combinadas para facilitar a memorizaç ão e melhorar a segurança. Se você optar por uma senha comum: - Ela precisa ser longa, com caracteres minúsculo s e maiúsculos, possivelmente também números e caracteres especiais . - Evite elementos óbvios, como “senha”, sequências de letras ou números como “abc”, números como “123”. - Evite usar informações pessoais que sejam encontradas on-line. E, se você usa códigos ou senhas, não as reutilize em outro lugar. - Não os compartilhe com colegas. - Habilite a Autenticação	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Multifatorial. - Use um gerenciador de senhas exclusivo.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5_PROTEJA O ACESSO AOS SISTEMAS	Incentive todos a usarem um código secreto com pelo menos três palavras comuns aleatória s combinadas para facilitar a memorizaç ão e melhorar a segurança. Se você optar por uma senha comum: - Ela precisa ser longa, com caracteres minúsculo s e maiúsculos, possivelmente também números e caracteres especiais . - Evite elementos óbvios, como “senha”, sequências de letras ou números como “abc”, números como “123”. - Evite usar informações pessoais que sejam encontradas on-line. E, se você usa códigos ou senhas, não as reutilize em outro lugar. - Não os compartilhe com colegas. - Habilite a Autenticação	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Multifatorial. - Use um gerenciador de senhas exclusivo.		
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_PROTEJA OS DISPOSITIVOS: MANTENHA O SOFTWARE ATUALIZADO E COM O PATCHES	O ideal é usar uma plataforma centralizada para gerenciar a aplicação de patches. É altamente recomendável que as PMEs: - Atualize regularmente todos os seus softwares. - Habilite as atualizações automáticas sempre que possível. - Identifique o software e o hardware que exijam atualizações manuais. - Considere os dispositivos móveis e de IoT.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	elasticsearch-encrypted-at-rest	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os domínios do Amazon Elasticsearch Service (Amazon ES).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	elasticsearch-node-to-node-encryption-check	Certifique-se de que a node-to-node criptografia para o Amazon Elasticsearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenad os em dispositi vos móveis, como laptops, smartphon es e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroporto s WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifiqu e-se de que os sites desses estabelec imentos estejam empregando tecnologi a de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenad os em dispositi vos móveis, como laptops, smartphon es e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroporto s WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifiqu e-se de que os sites desses estabelec imentos estejam empregando tecnologi a de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenad os em dispositi vos móveis, como laptops, smartphon es e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroporto s WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifiqu e-se de que os sites desses estabelec imentos estejam empregando tecnologi a de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6_DISPOSITIVOS SEGUROS: CRIPTOGRAFIA	Proteja os dados com criptografia. As PMEs devem garantir que os dados armazenados em dispositivos móveis, como laptops, smartphones e tabelas, sejam criptografados. Para dados transferidos por redes públicas, como redes de hotéis ou aeroportos WiFi , assegure-se de que os dados sejam criptografados, empregando uma Rede Privada Virtual (VPN) ou acessando sites por meio de conexões seguras usando o protocolo SSL/TLS. Certifique-se de que os sites desses estabelecimentos estejam empregando tecnologia de criptografia adequada para proteger os dados do cliente enquanto eles trafegam pela Internet.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	netfw-policy-rule-group-associated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: USE FIREWALLS	Os firewalls gerenciam o tráfego que entra e sai de uma rede e são uma ferramenta crítica na proteção dos sistemas de PMEs. Firewalls devem ser implantados para proteger todos os sistemas críticos, em particular, um firewall deve ser empregado para manter a rede da PME segura na Internet.	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferramentas de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determinados endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoramento e o alerta estejam ativados para avisar sobre ataques	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferramentas de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determinados endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoramento e o alerta estejam ativados para avisar sobre ataques	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferramentas de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determinados endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoramento e o alerta estejam ativados para avisar sobre ataques	elasticsearch-logs-to-cloudwatch	Garanta que os domínios do serviço Amazon Elasticsearch tenham registros de erros habilitados e transmitidos para o CloudWatch Amazon Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferramentas de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determinados endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoramento e o alerta estejam ativados para avisar sobre ataques	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferramentas de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determinados endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoramento e o alerta estejam ativados para avisar sobre ataques	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7_PROTEJA SUA REDE: ANALISE AS SOLUÇÕES DE ACESSO REMOTO	As PMEs devem revisar regularmente todas as ferrament as de acesso remoto para garantir que estejam seguras, em especial: - Certifique-se de que todo o software de acesso remoto esteja atualizado e tenha patches aplicados. - Restrinja o acesso remoto de localizações geográficas suspeitas ou de determina dos endereços IP. - Restrinja o acesso remoto da equipe somente aos sistemas e computadores necessários para o trabalho. - Aplique senhas fortes para acesso remoto e, sempre que possível, ative a autenticação multifatorial. - Garanta que o monitoram ento e o alerta estejam ativados para avisar sobre ataques	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	suspeitos ou atividades suspeitas incomuns.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomware. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadamente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularmente os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomware. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadamente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularmente os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomware. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadamente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularmente os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	ec2-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	fsx-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomware. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadamente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularmente os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9_PROTEJA OS BACKUPS	Para permitir a recuperação da formação de chaves, os backups devem ser mantidos, porque são uma forma eficaz de se recuperar de desastres, como um ataque de ransomwar e. É preciso aplicar as seguintes regras de backup: o backup deve ser regular e automatizado sempre que possível; o backup deve ser mantido separadam ente do ambiente de produção da PME; os backups deverão ser criptografados, especialmente se mudarem de local; a capacidade de restaurar regularme nte os dados dos backups é testada. Idealmente, deve ser feito um teste regular de uma restauração completa do início ao fim.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11_PROTEJA OS SITES ON-LINE	É essencial que as PMEs configurem e mantenham seus sites on-line com segurança e protejam adequadamente os dados pessoais ou detalhes financeir os, como informaçõ es de cartão de crédito. Isso implicará a execução de testes de segurança regulares nos sites para identificar possíveis brechas de segurança e a realização de análises periódica s para manter o site funcionan do e atualizado adequadamente.	vuln-management-pl an-exists (verificação de processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente.

Modelo

O modelo está disponível em GitHub: Guia de melhores práticas operacionais para a ENISA de cibersegurança para PME.

Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Low

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os controles de estrutura Low do Esquema Nacional de Seguridad (ENS) da Espanha e as regras gerenciadas AWS do Config. Cada regra de Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles ENS Low da Espanha. Um controle ENS da Espanha pode estar relacionado a várias regras de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do framework ENS Low da Espanha, conforme atualizado pela última vez em 23/10/2020.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a

ID de controle	AWS Regra de configuração	Orientação
		criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balancead or de carga seja excluído de forma acidental ou mal-inten cionada, o que pode levar à perda de disponibilidade das aplicações.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
Anexo II 4.1.2.b)	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.1.2.b)	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.2.1.a)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.1.a); b)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Anexo II 4.2.4	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.BAJO.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.BAJO.c)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Ative essa regra para restringi r o acesso aos recursos na AWS nuvem. Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
Anexo II 4.3.1	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.3.1	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.3.2.b)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 4.3.2.b)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
Anexo II 4.3.2.b)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.
Anexo II 4.3.2.b)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Anexo II 4.3.2.b)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabi lidades em seu ambiente. Isso pode incluir ferrament as de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloud watch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.3.8.BAJO	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.6.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.2.3	security-awareness-program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.BAJO.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Anexo II 5.7.3	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 5.7.3	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Anexo II 5.7.3	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
Anexo II 5.7.3	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.7.3	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
Anexo II 5.7.3	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
Anexo II 5.8.2	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.2	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Art. 14.4	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
Art. 16	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Art. 16	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
Art. 20.2	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferramentas de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Art. 21.1	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	elb-cross-zone-load-balanci ng-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Art. 21.1	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Art. 21.1	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
Art. 21.1	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Art. 21.1	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Art. 21.1	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Art. 21.1	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
Art. 21.1	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Art. 21.1	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Art. 21.1	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
Art. 22	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
Art. 22	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
Art. 22	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Art. 22	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Art. 22	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
Art. 22	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Art. 22	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
Art. 22	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
Art. 22	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.
Art. 23	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Art. 23	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Art. 23	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Art. 25	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
Art. 25	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
Art. 25	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o Esquema Nacional de Seguridad (ENS) Low.

Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Medium

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os controles da estrutura Medium do Esquema Nacional de Seguridad (ENS) da Espanha e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles ENS Medium da Espanha. Um controle ENS da Espanha pode estar relacionado a várias regras de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do framework ENS Medium da Espanha, conforme atualizado pela última vez em 23/10/2020.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a

ID de controle	AWS Regra de configuração	Orientação
		criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balancead or de carga seja excluído de forma acidental ou mal-inten cionada, o que pode levar à perda de disponibilidade das aplicações.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
Anexo II 4.1.2.b)	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.1.2.b)	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.2.1.a)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Anexo II 4.2.4	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.c)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.c)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.2.6.c)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.c)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.2.6.c)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.c)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
Anexo II 4.2.7	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
Anexo II 4.2.7	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
Anexo II 4.3.1	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.3.1	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.3.2.b)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
Anexo II 4.3.2.b)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Anexo II 4.3.2.b)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectado s somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabi lidades em seu ambiente. Isso pode incluir ferrament as de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.
Anexo II 4.3.6	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.7.a)	response-plan-exists-mainta ined (Verificação do processo)	Garanta que os planos de resposta a incidente s sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.
Anexo II 4.3.8	elasticsearch-logs-to-cloud watch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.3.8	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.3.8	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.3.8	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
Anexo II 4.3.8	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.6.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Anexo II 4.6.2	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.6.2	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Anexo II 5.2.3	security-awareness-program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.4.2	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.4.2	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.4.3	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.4.3	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Anexo II 5.7.3	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 5.7.3	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Anexo II 5.7.3	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
Anexo II 5.7.3	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.7.3	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
Anexo II 5.7.3	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
Anexo II 5.8.2	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.2	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 5.8.3.b)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.b)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 5.8.3.b)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.b)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.b)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
Art. 14.4	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
Art. 16	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Art. 16	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
Art. 20.2	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferramentas de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Art. 21.1	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Art. 21.1	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Art. 21.1	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Art. 21.1	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Art. 21.1	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Art. 21.1	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
Art. 21.1	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Art. 21.1	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Art. 21.1	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
Art. 22	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
Art. 22	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Art. 22	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
Art. 22	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectado s somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Art. 22	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
Art. 22	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Art. 22	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
Art. 22	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
Art. 22	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Art. 23	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Art. 23	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Art. 23	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Art. 24.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
Art. 24.2	response-plan-exists-mainta ined (Verificação do processo)	Garanta que os planos de resposta a incidente s sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.
Art. 25	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
Art. 25	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
Art. 25	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o Esquema Nacional de Seguridad (ENS) Medium.

Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) High

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os controles de estrutura High do Esquema Nacional de Seguridad (ENS) da Espanha e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles ENS High da Espanha. Um controle ENS da Espanha pode estar relacionado a várias regras de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do framework ENS High da Espanha, conforme atualizado pela última vez em 09/07/2021.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed (Verificação do processo)	Faça uma avaliação anual de risco em sua organizaç ão. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.
4.2.1.b)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management

ID de controle	AWS Regra de configuração	Orientação
		(IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
4.2.5.ALTO.a)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balancead or de carga seja excluído de forma acidental ou mal-inten cionada, o que pode levar à perda de disponibilidade das aplicações.
Anexo II 4.1.2.a); b); c)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
Anexo II 4.1.2.b)	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.1.2.b)	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.2.1.a)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.4	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
Anexo II 4.2.5	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.BAJO.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.5.BAJO.c)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloud watch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
Anexo II 4.3.1	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
Anexo II 4.3.1	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.1	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
Anexo II 4.3.2.b)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 4.3.2.b)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.
Anexo II 4.3.2.b)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectado s somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Anexo II 4.3.2.b)	lambda-function-public-acce ss-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Anexo II 4.3.2.b)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
Anexo II 4.3.4.c)	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabi lidades em seu ambiente. Isso pode incluir ferrament as de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.6	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained (Verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.3.8.BAJO	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Anexo II 4.3.8.MEDIO	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 4.3.8.MEDIO	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.6.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.2.3	security-awareness-program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
Anexo II 5.2.4	security-awareness-program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
Anexo II 5.2.5	security-awareness-program-exists (Verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2.MEDIO	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2.MEDIO	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.2.MEDIO	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.BAJO.a)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3.MEDIO	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3.MEDIO	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.4.3.MEDIO	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub
Anexo II 5.7.3	dynamodb-table-encrypted-km s	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	sagemaker-notebook-instance -kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo II 5.7.3	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Anexo II 5.7.3	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo II 5.7.3	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Anexo II 5.7.3	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
Anexo II 5.7.3	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo II 5.7.3	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Anexo II 5.7.3	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
Anexo II 5.7.3	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
Anexo II 5.7.3	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
Anexo II 5.7.3	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
Anexo II 5.8.2	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.2	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
Art. 14.4	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
Art. 16	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Art. 16	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Art. 16	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 20.2	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
Art. 20.2	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferramentas de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
Art. 21.1	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidad e da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
Art. 21.1	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
Art. 21.1	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
Art. 21.1	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Art. 21.1	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Art. 21.1	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
Art. 21.1	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
Art. 21.1	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Art. 21.1	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Art. 21.1	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
Art. 21.1	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
Art. 21.1	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Art. 21.1	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
Art. 21.1	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
Art. 22	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
Art. 22	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
Art. 22	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Art. 22	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Art. 22	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
Art. 22	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
Art. 22	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
Art. 22	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Art. 22	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Art. 22	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
Art. 22	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
Art. 22	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
Art. 23	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitad os e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Art. 23	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Art. 23	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
Art. 23	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
Art. 23	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Art. 23	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Art. 23	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Art. 24.2	response-plan-exists-maintained (Verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.

ID de controle	AWS Regra de configuração	Orientação
Art. 24.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Art. 25	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Art. 25	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
Art. 25	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
Art. 25	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
Art. 25	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
Art. 25	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o Esquema Nacional de Seguridad (ENS) High.

Operational Best Practices for FDA Title 21 CFR Part 11

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Título 21 do Código de Regulamentos Federais (CFR), Parte 11, e as regras AWS gerenciadas do Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles do Título 21 CFR Parte 11 da FDA. O controle do Título 21 CFR Parte 11 da FDA pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:		os para atender aos requisitos de resiliênc ia.
11.1	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.1	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte:	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja habilitada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(a)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (a) Validação de sistemas para garantir precisão, confiabilidade, desempenho consistente pretendido e a capacidade de reconhecer registros inválidos ou alterados.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	ecr-private-lifecycle-policy-configured	As políticas de ciclo de vida do Amazon Elastic Container Repository (ECR) permitem que você especifique o gerenciamento do ciclo de vida das imagens em um repositório. Isso permite a automação da limpeza de imagens não usadas, como imagens prestes a expirar com base em seu tempo de vida ou contagem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(c)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (c) Proteção de registros para permitir sua recuperação precisa e imediata durante todo o período de retenção de registros.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(d)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (d) Limitar o acesso ao sistema a indivíduos autorizados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônicos. As alterações no registro não devem obscurecer as informações registradas anteriormente. Essa documentação da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedime ntos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônicos. As alterações no registro não devem obscurecer as informações registradas anteriormente. Essa documentação da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônicos. As alterações no registro não devem obscurecer as informações registradas anteriormente. Essa documentação da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônicos. As alterações no registro não devem obscurecer as informações registradas anteriormente. Essa documentação da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedime ntos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(e)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (e) Uso de trilhas de auditoria seguras, geradas por computador e com registro de data e hora para registrar de forma independente a data e a hora das entradas e ações do operador que criam, modificam ou excluem	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	registros eletrônic os. As alteraçõe s no registro não devem obscurecer as informações registrad as anteriormente. Essa documenta ção da trilha de auditoria deve ser retida por um período pelo menos igual ao exigido para os registros eletrônicos em questão e deve estar disponível para revisão e cópia pela agência.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		ser atribuídas a uma VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizados possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(g)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (g) Uso de verificações de autoridade para garantir que somente indivíduos autorizad os possam usar o sistema, assinar eletronicamente um registro, acessar a operação ou o dispositivo de entrada ou saída do sistema	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de computador, alterar um registro ou realizar a operação em questão.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(h)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (h) Uso de verificações do dispositivo (por exemplo, terminal) para determinar, conforme apropriado, a validade da fonte de entrada de dados ou instrução operacional.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(h)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (h) Uso de verificações do dispositivo (por exemplo, terminal) para determinar, conforme apropriado, a validade da fonte de entrada de dados ou instrução operacional.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(h)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (h) Uso de verificações do dispositivo (por exemplo, terminal) para determinar, conforme apropriado, a validade da fonte de entrada de dados ou instrução operacional.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(i)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (i) Determinação de que as pessoas que desenvolvem, mantêm ou usam sistemas de registro eletrônico/assinatura eletrônica tenham educação, treinamento e experiência para realizar as tarefas que	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	foram atribuídas a elas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo : (1) Controles adequados sobre a distribuição, acesso e uso da documenta ção para operação e manutenção do sistema. (2)	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo : (1) Controles adequados sobre a distribuição, acesso e uso da documenta ção para operação e manutenção do sistema. (2)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documenta ção dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo : (1) Controles adequados sobre a distribuição, acesso e uso da documenta ção para operação e manutenção do sistema. (2)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo : (1) Controles adequados sobre a distribuição, acesso e uso da documenta ção para operação e manutenção do sistema. (2)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamen te o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo : (1) Controles adequados sobre a distribuição, acesso e uso da documenta ção para operação e manutenção do sistema. (2)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documenta ção dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.10(k)	Pessoas que usam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos, e para garantir que o signatário não possa repudiar prontamente o registro assinado como não genuíno. Esses procedimentos e controles devem incluir o seguinte: (k) Uso de controles apropriados sobre a documentação dos sistemas, incluindo: (1) Controles adequados sobre a distribuição, acesso e uso da documentação para operação e manutenção do sistema. (2)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Procedimentos de revisão e controle de alterações para manter uma trilha de auditoria que documente o desenvolvimento e a modificação sequenciados no tempo da documentação dos sistemas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlad o ao sistema, cada assinatura deve ser executada usando todos os component es da assinatura eletrônica. (2) Ser usado somente por seus proprietá rios autênticos; e (3) Ser administr ado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietá rio genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado ao sistema, cada assinatura deve ser executada usando todos os componentes da assinatura eletrônica. (2) Ser usado somente por seus proprietários autênticos; e (3) Ser administrado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de duas ou mais pessoas.		o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlad o ao sistema, cada assinatura deve ser executada usando todos os component es da assinatura eletrônica. (2) Ser usado somente por seus proprietá rios autênticos; e (3) Ser administr ado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietá rio genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado ao sistema, cada assinatura deve ser executada usando todos os componentes da assinatura eletrônica. (2) Ser usado somente por seus proprietários autênticos; e (3) Ser administrado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado ao sistema, cada assinatura deve ser executada usando todos os componentes da assinatura eletrônica. (2) Ser usado somente por seus proprietários autênticos; e (3) Ser administrado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado ao sistema, cada assinatura deve ser executada usando todos os componentes da assinatura eletrônica. (2) Ser usado somente por seus proprietários autênticos; e (3) Ser administrado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.2	(a) As assinaturas eletrônicas que não são baseadas em biometria devem: (1) Empregar pelo menos dois component es de identificação distintos, como um código de identific ação e uma senha. (i) Quando um indivíduo executa uma série de assinaturas durante um único período contínuo de acesso controlad o ao sistema, a primeira assinatura deve ser executada usando todos os componentes da assinatura eletrônic a; as assinaturas subsequentes devem ser executadas usando pelo menos um componente de assinatura eletrônic a que só é executáve l e projetado para ser usado somente pelo indivíduo. (ii) Quando um indivíduo	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	executa uma ou mais assinaturas não executadas durante um único período contínuo de acesso controlado ao sistema, cada assinatura deve ser executada usando todos os componentes da assinatura eletrônica. (2) Ser usado somente por seus proprietários autênticos; e (3) Ser administrado e executado para garantir que a tentativa de uso da assinatura eletrônica de um indivíduo por qualquer pessoa que não seja seu proprietário genuíno exija a colaboração de duas ou mais pessoas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	[api-gw-cache-enabled-and-encrypted](https://)	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja habilitada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar , manter ou transmiti r registros eletrônic os devem empregar procedimentos e controles projetado s para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimen to. Esses procedime ntos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriad os de assinatura digital para garantir, conforme necessári o, dadas as circunstâ ncias, a autentici dade, integridade e	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.3	Pessoas que usam sistemas abertos para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles projetados para garantir a autenticidade, integridade e, quando apropriado, a confidencialidade dos registros eletrônicos desde o ponto de sua criação até o ponto de seu recebimento. Esses procedimentos e controles devem incluir aqueles identificados em 11.10, conforme apropriado, e medidas adicionais, como criptografia de documentos e uso de padrões apropriados de assinatura digital para garantir, conforme necessário, dadas as circunstâncias, a autenticidade, integridade e	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	confidencialidade dos registros.		
11.300(b)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperad as ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(b)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperad as ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(b)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperad as ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(b)	Pessoas que usam assinaturas eletrônicas com base no uso de códigos de identificação em combinação com senhas devem empregar controles para garantir sua segurança e integridade. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperadas ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(b)	Pessoas que usam assinaturas eletrônicas com base no uso de códigos de identificação em combinação com senhas devem empregar controles para garantir sua segurança e integridade. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperadas ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(b)	Pessoas que usam assinaturas eletrônicas com base no uso de códigos de identificação em combinação com senhas devem empregar controles para garantir sua segurança e integridade. Esses controles devem incluir: (b) Garantir que as emissões de códigos de identificação e senhas sejam verificadas, recuperadas ou revisadas periodicamente (por exemplo, para cobrir eventos como o envelhecimento da senha).	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(d)	Pessoas que usam assinaturas eletrônicas com base no uso de códigos de identificação em combinação com senhas devem empregar controles para garantir sua segurança e integridade. Esses controles devem incluir: (d) O uso de proteções de transação para evitar o uso não autorizado de senhas e/ou códigos de identificação e para detectar e relatar de forma imediata e urgente quaisquer tentativas de seu uso não autorizado à unidade de segurança do sistema e, conforme apropriado, à gerência organizacional.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(d)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (d) O uso de proteções de transação para evitar o uso não autorizad o de senhas e/ou códigos de identific ação e para detectar e relatar de forma imediata e urgente quaisquer tentativa s de seu uso não autorizado à unidade de segurança do sistema e, conforme apropriado, à gerência organizac ional.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(d)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (d) O uso de proteções de transação para evitar o uso não autorizad o de senhas e/ou códigos de identific ação e para detectar e relatar de forma imediata e urgente quaisquer tentativa s de seu uso não autorizado à unidade de segurança do sistema e, conforme apropriado, à gerência organizac ional.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.300(d)	Pessoas que usam assinaturas eletrônic as com base no uso de códigos de identific ação em combinaçã o com senhas devem empregar controles para garantir sua segurança e integrida de. Esses controles devem incluir: (d) O uso de proteções de transação para evitar o uso não autorizad o de senhas e/ou códigos de identific ação e para detectar e relatar de forma imediata e urgente quaisquer tentativa s de seu uso não autorizado à unidade de segurança do sistema e, conforme apropriado, à gerência organizac ional.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o Título 21 CFR Parte 11 da FDA.

Práticas recomendadas operacionais para o FedRAMP (Baixo)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre os controles básicos baixos do Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP) e AWS as regras gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do FedRAMP. Um controle do FedRAMP pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
AC-2	GERENCIAMENTO DA CONTA	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-2	GERENCIAMENTO DA CONTA	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC-2	GERENCIAMENTO DA CONTA	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	GERENCIAMENTO DA CONTA	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-3	FISCALIZAÇÃO DE ACESSO	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-3	FISCALIZAÇÃO DE ACESSO	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-3	FISCALIZAÇÃO DE ACESSO	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-3	FISCALIZAÇÃO DE ACESSO	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-3	FISCALIZAÇÃO DE ACESSO	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-3	FISCALIZAÇÃO DE ACESSO	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	FISCALIZAÇÃO DE ACESSO	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-3	FISCALIZAÇÃO DE ACESSO	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17	ACESSO REMOTO	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17	ACESSO REMOTO	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-17	ACESSO REMOTO	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-17	ACESSO REMOTO	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-17	ACESSO REMOTO	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-17	ACESSO REMOTO	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-17	ACESSO REMOTO	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17	ACESSO REMOTO	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17	ACESSO REMOTO	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-2	EVENTOS DA AUDITORIA	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-2	EVENTOS DA AUDITORIA	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	EVENTOS DA AUDITORIA	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	CONTEÚDO DOS REGISTROS DE AUDITORIA	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6	REVISÃO, ANÁLISE E GERAÇÃO DE RELATÓRIOS DE AUDITORIA	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	PROTEÇÃO DE INFORMAÇÕES DE AUDITORIA	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
AU-9	PROTEÇÃO DE INFORMAÇÕES DE AUDITORIA	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	PROTEÇÃO DE INFORMAÇÕES DE AUDITORIA	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	PROTEÇÃO DE INFORMAÇÕES DE AUDITORIA	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AU-9	PROTEÇÃO DE INFORMAÇÕES DE AUDITORIA	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-11	RETENÇÃO DE REGISTROS DE AUDITORIA	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-12	GERAÇÃO DE AUDITORIA	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-12	GERAÇÃO DE AUDITORIA	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	GERAÇÃO DE AUDITORIA	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
CA-7	MONITORAMENTO CONTÍNUO	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
CA-7	MONITORAMENTO CONTÍNUO	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CA-7	MONITORAMENTO CONTÍNUO	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	MONITORAMENTO CONTÍNUO	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais e o controle de acesso é necessário para essas contas.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	CONFIGURAÇÃO DE REFERÊNCIA	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.
CM-7	FUNCIONALIDADE MÍNIMA	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7	FUNCIONALIDADE MÍNIMA	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7	FUNCIONALIDADE MÍNIMA	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	INVENTÁRIO DE COMPONENTES DO SISTEMA DE INFORMAÇÃO	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	INVENTÁRIO DE COMPONENTES DO SISTEMA DE INFORMAÇÃO	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	INVENTÁRIO DE COMPONENTES DO SISTEMA DE INFORMAÇÃO	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	INVENTÁRIO DE COMPONENTES DO SISTEMA DE INFORMAÇÃO	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	BACKUP DO SISTEMA DE INFORMAÇÃO	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	RECONSTITUIÇÃO E RECUPERAÇÃO DO SISTEMA DE INFORMAÇÃO	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	IDENTIFICAÇÃO E AUTENTICAÇÃO (USUÁRIOS ORGANIZACIONAIS)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5	GERENCIAMENTO DE AUTENTICADORES	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5	GERENCIAMENTO DE AUTENTICA DORES	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4	TRATAMENTO DE INCIDENTES	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4	TRATAMENTO DE INCIDENTES	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4	TRATAMENTO DE INCIDENTES	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4	TRATAMENTO DE INCIDENTES	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4	TRATAMENTO DE INCIDENTES	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6	RELATÓRIOS DE INCIDENTES	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6	RELATÓRIOS DE INCIDENTES	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6	RELATÓRIOS DE INCIDENTES	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7	ASSISTÊNCIA NA RESPOSTA A INCIDENTES	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7	ASSISTÊNCIA NA RESPOSTA A INCIDENTES	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7	ASSISTÊNCIA NA RESPOSTA A INCIDENTES	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5	VERIFICAR VULNERABILIDADE	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5	VERIFICAR VULNERABILIDADE	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5	VERIFICAR VULNERABILIDADE	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3	CICLO DE VIDA DE DESENVOLVIMENTO DO SISTEMA	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3	CICLO DE VIDA DE DESENVOLVIMENTO DO SISTEMA	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3	CICLO DE VIDA DE DESENVOLVIMENTO DO SISTEMA	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	PROTEÇÃO CONTRA NEGAÇÃO DE SERVIÇO	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
SC-7	PROTEÇÃO DE LIMITES	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7	PROTEÇÃO DE LIMITES	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-7	PROTEÇÃO DE LIMITES	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7	PROTEÇÃO DE LIMITES	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7	PROTEÇÃO DE LIMITES	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7	PROTEÇÃO DE LIMITES	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-7	PROTEÇÃO DE LIMITES	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	PROTEÇÃO DE LIMITES	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
SC-12	GERENCIAMENTO E ESTABELECIMENTO DE CHAVES CRIPTOGRÁFICAS	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	GERENCIAMENTO E ESTABELECIMENTO DE CHAVES CRIPTOGRÁFICAS	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	GERENCIAMENTO E ESTABELECIMENTO DE CHAVES CRIPTOGRÁFICAS	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	PROTEÇÃO CRIPTOGRÁFICA	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	PROTEÇÃO CRIPTOGRÁFICA	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	PROTEÇÃO CRIPTOGRÁFICA	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	PROTEÇÃO CRIPTOGRÁFICA	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	PROTEÇÃO CRIPTOGRÁFICA	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	PROTEÇÃO CRIPTOGRÁFICA	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	REMEDIAÇÃO DE FALHAS	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	REMEDIAÇÃO DE FALHAS	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	REMEDIAÇÃO DE FALHAS	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	REMEDIAÇÃO DE FALHAS	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3	REMEDIAÇÃO DE FALHAS	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3	REMEDIAÇÃO DE FALHAS	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub
SI-3	REMEDIAÇÃO DE FALHAS	ecs-task-definition-memory-hard-limit	Limitar a memória máxima disponíve l para contêineres do Amazon Elastic Container Service (ECS) garante que não haja abuso no uso do recurso em caso de acesso mal-intencionado aos contêineres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	MONITORAMENTO DO SISTEMA DE INFORMAÇÃO	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	ALERTAS, RECOMENDAÇÕES E DIRETRIZES DE SEGURANÇA	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	ALERTAS, RECOMENDAÇÕES E DIRETRIZES DE SEGURANÇA	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	ALERTAS, RECOMENDAÇÕES E DIRETRIZES DE SEGURANÇA	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	ALERTAS, RECOMENDAÇÕES E DIRETRIZES DE SEGURANÇA	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	MANUSEIO E RETENÇÃO DE INFORMAÇÕES	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-16	PROTEÇÃO DE MEMÓRIA	ecs-task-definition-memory-hard-limit	Limitar a memória máxima disponíve l para contêineres do Amazon Elastic Container Service (ECS) garante que não haja abuso no uso do recurso em caso de acesso mal-intencionado aos contêineres.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o FedRAMP (Low).

Operational Best Practices for FedRAMP(Moderate)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do FedRAMP. Um controle do FedRAMP pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse pacote de conformidade foi validado pela AWS Security Assurance Services LLC (AWS SAS), que é uma equipe de avaliadores de segurança qualificados do setor de cartões de pagamento

(QSAs), profissionais certificados pela HITRUST Common Security Framework (CCSFPs) e profissionais de conformidade certificados para fornecer orientação e avaliações para várias estruturas do setor. AWS Os profissionais do SAS criaram esse pacote de conformidade para permitir que o cliente se alinhe a um subconjunto dos controles do FedRAMP.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(3)	O sistema de informações desativa automaticamente contas inativas após 90 dias para os usuários.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(3)	O sistema de informações desativa automaticamente contas inativas após 90 dias para os usuários.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(7)	A organização: (a) Estabelece e administra os usuários privilegiados de acordo com um esquema de acesso baseado em perfil que organiza o acesso e os privilégios permitidos ao sistema de informações em perfis; (b) Monitora as atribuições de perfis privilegiados; e (c) Executa [Atribuição: ações definidas pela organização] quando as atribuições de perfis privilegiados não são mais adequadas. Orientação complementar: perfis privilegiados são perfis definidos pela organização e atribuídos a indivíduos. Esses perfis permitem que os indivíduos desempenhem determinadas funções relevantes à segurança que	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários comuns não possuem autorização para realizar. Essas funções privilegiadas incluem, por exemplo, o gerenciamento de chaves e contas, a administração de rede e sistema, a administr ação do banco de dados da web.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(12)(a)	A organização: a. Monitora as contas do sistema de informações em busca de [Atribuição: uso atípico definido pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(12)(a)	A organização: a. Monitora as contas do sistema de informaçõ es em busca de [Atribuição: uso atípico definido pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformid ade com os requisito s de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformid ade com os requisito s de gerenciamento de contas [Atribuição: frequência definida pela organização].	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
AC-6(10)	O sistema de informações impede que usuários não privilegiados executem funções privilegiadas, incluindo desabilitar, contornar ou alterar as proteções ou contramedidas de segurança implementadas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(10)	O sistema de informações impede que usuários não privilegiados executem funções privilegiadas, incluindo desabilitar, contornar ou alterar as proteções ou contramedidas de segurança implement adas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(10)	O sistema de informações impede que usuários não privilegiados executem funções privilegiadas, incluindo desabilitar, contornar ou alterar as proteções ou contramedidas de segurança implement adas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informaçõ es pode auditar os seguintes eventos: eventos de login de conta bem-suced idos e com falha, eventos de gerenciam ento de contas, acesso a objetos, alterações de política, funções de privilégi o, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividade s do administrador, verificações de autenticação, verificaç ões de autorizaç ão, exclusões de dados, acesso a dados, alterações de dados e alteraçõe s de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatc h ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informaçõ es detalhadas sobre o projeto de compilaçã o.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informaçõ es pode auditar os seguintes eventos: eventos de login de conta bem-suced idos e com falha, eventos de gerenciam ento de contas, acesso a objetos, alterações de política, funções de privilégi o, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividade s do administrador, verificações de autenticação, verificaç ões de autorizaç ão, exclusões de dados, acesso a dados, alterações de dados e alteraçõe s de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informaçõ es pode auditar os seguintes eventos: eventos de login de conta bem-suced idos e com falha, eventos de gerenciam ento de contas, acesso a objetos, alterações de política, funções de privilégi o, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividade s do administrador, verificações de autenticação, verificaç ões de autorizaç ão, exclusões de dados, acesso a dados, alterações de dados e alteraçõe s de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informaçõ es pode auditar os seguintes eventos: eventos de login de conta bem-suced idos e com falha, eventos de gerenciam ento de contas, acesso a objetos, alterações de política, funções de privilégi o, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividade s do administrador, verificações de autenticação, verificaç ões de autorizaç ão, exclusões de dados, acesso a dados, alterações de dados e alteraçõe s de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2(a)(d)	A organização: (a) Determina se o sistema de informações pode auditar os seguintes eventos: eventos de login de conta bem-sucedidos e com falha, eventos de gerenciamento de contas, acesso a objetos, alterações de política, funções de privilégio, rastreamento de processos e eventos do sistema. Para aplicações da Web: todas as atividades do administrador, verificações de autenticação, verificações de autorização, exclusões de dados, acesso a dados, alterações de dados e alterações de permissão. (d) Determina que os seguintes eventos devem ser auditados dentro do sistema de informações: [subconjunto definido	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização dos eventos auditáveis definidos no AU-2a a ser auditado continuamente para cada evento identific ado].		
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatc h ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informaçõ es detalhadas sobre o projeto de compilaçã o.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
AU-7(1)	O sistema de informações fornece recursos para processar registros de auditoria para eventos de interesse com base em [Atribuição: campos de auditoria definidos pela organização nos registros de auditoria].	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-7(1)	O sistema de informações fornece recursos para processar registros de auditoria para eventos de interesse com base em [Atribuição: campos de auditoria definidos pela organização nos registros de auditoria].	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9(2)	O sistema de informações faz backup dos registros de auditoria no mínimo semanalme nte em um sistema ou componente de sistema fisicamente diferente do sistema ou do component e que está sendo auditado.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9(2)	O sistema de informações faz backup dos registros de auditoria no mínimo semanalme nte em um sistema ou componente de sistema fisicamente diferente do sistema ou do component e que está sendo auditado.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.
AU-9	O sistema de informações protege as informações e as ferramentas de auditoria contra acessos, modificaç ões e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	O sistema de informações protege as informações e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	O sistema de informações protege as informações e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
AU-11	A organização retém registros de auditoria por pelo menos 90 dias para fornecer suporte às after-the-fact investigações de incidentes de segurança e atender aos requisitos regulatórios e organizacionais de retenção de informações.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidad e de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os component es do sistema de informações e da rede em que a capacidad e de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidad e de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os component es do sistema de informações e da rede em que a capacidad e de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidad e de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os component es do sistema de informações e da rede em que a capacidad e de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos em AU-2 (a) em todos os componentes do sistema de informações e da rede em que a capacidade de auditoria está implantada ou disponível (c) Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	rds-enhanced-monit oring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibi lidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	dynamodb-throughpu t-limit-check	Habilite essa regra para garantir que a capacidade de throughput provision ada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidad e de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalm ente os parâmetro s AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentag e (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organização desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
CM-2	A organização desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restaurav eis publicamente. Os snapshots de volume do EBS podem conter informaçõ es confidenciais e o controle de acesso é necessário para essas contas.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-instance-no-pu blic-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organização desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada . Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.
CM-7 (a)	A organização: a. Configura o sistema de informações para fornecer somente os recursos essenciais.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7 (a)	A organização: a. Configura o sistema de informações para fornecer somente os recursos essenciais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7(a)	A organização: a. Configura o sistema de informações para fornecer somente os recursos essenciais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(1)	A organização atualiza o inventário dos componentes do sistema de informações como parte integrante das instalações, remoções e atualizações do sistema de informações.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(1)	A organização atualiza o inventário dos componentes do sistema de informações como parte integrante das instalações, remoções e atualizações do sistema de informações.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)(a)	A organização: (a) Emprega mecanismos automatizados continuamente, usando mecanismos automatizados com um atraso máximo de cinco minutos na detecção, para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)(a)	A organização: (a) Emprega mecanismos automatizados continuamente, usando mecanismos automatizados com um atraso máximo de cinco minutos na detecção, para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)(a)	A organização: (a) Emprega mecanismos automatizados continuamente, usando mecanismos automatizados com um atraso máximo de cinco minutos na detecção, para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)(a)	A organização: (a) Emprega mecanismos automatizados continuamente, usando mecanismos automatizados com um atraso máximo de cinco minutos na detecção, para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9(b)	A organização: (b) Realiza backups de informações no nível de sistema contidas no sistema de informações (incrementais diárias e completas semanalmente).	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperaç ão e a reconstit uição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)(2)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)(2)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)(2)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)(2)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	O sistema de informações identifica e autentica de forma exclusiva os usuários organizacionais (ou processos que atuam em nome dos usuários organizacionais).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2	O sistema de informações identifica e autentica de forma exclusiva os usuários organizacionais (ou processos que atuam em nome dos usuários organizacionais).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)(a)(d)(e)	O sistema de informação, para autenticação baseada em senha: (a) Impõe a complexidade mínima da senha de [Atribuição: requisitos definidos pela organização para diferenciação de maiúsculas e minúsculas, número de caracteres, combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais, incluindo requisitos mínimos para cada tipo]; (d) Impõe restrições de vida útil mínima e máxima da senha de [Atribuição: números definidos pela organização para a vida útil mínima e a vida útil máxima]; (e) Proíbe a reutilização de senhas por 24 gerações	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(4)	A organização emprega ferrament as automatizadas para determina r se os autentica dores de senha são suficientemente fortes para satisfazer a [Atribuição: requisito s definidos pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(7)	A organização garante que autenticadores estáticos não criptografados não sejam incorporados em aplicações ou scripts de acesso, nem armazenados em teclas de função.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6(1)	A organização emprega mecanismos automatizados para ajudar a comunicar incidentes de segurança.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6(1)	A organização emprega mecanismos automatizados para ajudar a comunicar incidentes de segurança.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-6(1)	A organização emprega mecanismos automatizados para ajudar a comunicar incidentes de segurança.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7(1)	A organização emprega mecanismos automatizados para aumentar a disponibilidade de informações e suporte relacionados à resposta a incidentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7(1)	A organização emprega mecanismos automatizados para aumentar a disponibilidade de informações e suporte relacionados à resposta a incidentes.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-7(1)	A organização emprega mecanismos automatizados para aumentar a disponibilidade de informações e suporte relacionados à resposta a incidentes.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5(1)	A organização emprega ferrament as de verificações de vulnerabilidades que incluem a capacidad e de prontamente atualizar as vulnerabi lidades do sistema de informações que devem ser verificad as. Orientação complementar: as vulnerabilidades de devem ser verificad as precisam ser prontamente atualizad as à medida que novas vulnerabi lidades são descobert as e anunciadas e métodos de verificaç ão são desenvolvidos. Esse processo de atualização ajuda a garantir que possíveis vulnerabilidades no sistema de informaçõ es sejam identific adas e corrigidas o mais rápido possível. Controles relaciona dos: SI-3, SI-7.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5(1)	A organização emprega ferramentas de verificações de vulnerabilidades que incluem a capacidade de prontamente atualizar as vulnerabilidades do sistema de informações que devem ser verificadas. Orientação complementar: as vulnerabilidades de devem ser verificadas precisam ser prontamente atualizadas à medida que novas vulnerabilidades são descobertas e anunciadas e métodos de verificação são desenvolvidos. Esse processo de atualização ajuda a garantir que possíveis vulnerabilidades no sistema de informações sejam identificadas e corrigidas o mais rápido possível. Controles relacionados: SI-3, SI-7.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5(1)	A organização emprega ferrament as de verificações de vulnerabilidades que incluem a capacidad e de prontamente atualizar as vulnerabi lidades do sistema de informações que devem ser verificad as. Orientação complementar: as vulnerabilidades de devem ser verificad as precisam ser prontamente atualizad as à medida que novas vulnerabi lidades são descobert as e anunciadas e métodos de verificaç ão são desenvolvidos. Esse processo de atualização ajuda a garantir que possíveis vulnerabilidades no sistema de informaçõ es sejam identific adas e corrigidas o mais rápido possível. Controles relaciona dos: SI-3, SI-7.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5	A organização: (a) Verifica mensalmente as vulnerabilidades presentes no sistema de informações e nas aplicações hospedadas [sistema ou infraestrutura operacional; mensalmente em aplicações web e bancos de dados] quando novas vulnerabilidades que potencialmente afetam o sistema ou aplicações são identificadas e reportadas; (b) Emprega ferramentas e técnicas de verificação de vulnerabilidades que facilitam a interoperabilidade entre ferramentas e automatizam partes do processo de gerenciamento de vulnerabilidades usando padrões para: 1. Enumerar plataformas, falhas de software e configurações impróprias;	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	2. Formatar listas de verificação e procedimentos de teste; e 3. Medir o impacto da vulnerabilidade; (c) Analisa relatórios de verificação de vulnerabilidade e resultados de avaliações de controle de segurança; (d) Corrige vulnerabilidades legítimas: vulnerabilidades de alto risco são mitigadas em trinta (30) dias a partir da data da descoberta; vulnerabilidades de risco moderado são mitigadas em noventa (90) dias a partir da data da descoberta; vulnerabilidades de baixo risco são mitigadas em cento e oitenta (180) dias a partir da data da descoberta, de acordo com uma avaliação organizacional de risco; e (e) Compartilha as informações obtidas no processo		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de verificação de vulnerabilidades e nas avaliações de controle de segurança com [Atribuição: pessoal ou perfis definidos pela organização] para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informações (ou seja, fraquezas ou deficiências sistêmica s).		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5	A organização: a. Verifica vulnerabilidades presentes no sistema de informações e nas aplicações hospedadas [Atribuição: frequência definida pela organização e/ou aleatoriamente, de acordo com o processo definido pela organização] e quando novas vulnerabilidades que potencialmente afetam o sistema ou aplicações são identificadas e reportadas; (b) Emprega ferramentas e técnicas de verificação de vulnerabilidades que facilitam a interoperabilidade entre ferramentas e automatizam partes do processo de gerenciamento de vulnerabilidades usando padrões para: 1. Enumerar plataformas, falhas de	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	software e configura ções impróprias; 2. Formatar listas de verificação e procedimentos de teste; e 3. Medir o impacto da vulnerabi lidade; (c) Analisa relatórios de verificaç ão de vulnerabi lidade e resultado s de avaliações de controle de segurança ; (d) Corrige vulnerabi lidades legítimas [Atribuição: tempos de resposta definidos pela organização], de acordo com uma avaliação organizac ional de risco; e (e) Compartilha as informações obtidas no processo de verificação de vulnerabilidades e nas avaliações de controle de segurança com [Atribuição: pessoal ou perfis definidos pela organização] para ajudar a eliminar vulnerabilidades semelhantes em		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	outros sistemas de informações (ou seja, fraquezas ou deficiências sistêmicas).		
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10	A organização exige que o desenvolvedor do sistema de informações, do componente do sistema ou serviço do sistema de informações: (a) Execute o gerenciamento de configuração durante o desenvolvimento, a implementação e a operação do sistema, do componente ou do serviço; (b) Documente, gerencie e controle a integridade das alterações em [Atribuição: itens de configuração definidos pela organização sob gerenciamento de configuração]; (c) Implemente somente as alterações aprovadas pela organização no sistema, no componente ou no serviço; (d) Documente as alterações aprovadas	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10	A organização exige que o desenvolv edor do sistema de informações, do componente do sistema ou serviço do sistema de informaçõ es: (a) Execute o gerenciamento de configuração durante o desenvolvimento, a implementação e a operação do sistema, do componente ou do serviço; (b) Documente, gerencie e controle a integrida de das alteraçõe s em [Atribuição: itens de configura ção definidos pela organização sob gerenciamento de configuração]; (c) Implement e somente as alterações aprovadas pela organizaç ão no sistema, no componente ou no serviço; (d) Documente as alterações aprovadas	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10	A organização exige que o desenvolvedor do sistema de informações, do componente do sistema ou serviço do sistema de informações: (a) Execute o gerenciamento de configuração durante o desenvolvimento, a implementação e a operação do sistema, do componente ou do serviço; (b) Documente, gerencie e controle a integridade das alterações em [Atribuição: itens de configuração definidos pela organização sob gerenciamento de configuração]; (c) Implemente somente as alterações aprovadas pela organização no sistema, no componente ou no serviço; (d) Documente as alterações aprovadas	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10	A organização exige que o desenvolv edor do sistema de informações, do componente do sistema ou serviço do sistema de informaçõ es: (a) Execute o gerenciamento de configuração durante o desenvolvimento, a implementação e a operação do sistema, do componente ou do serviço; (b) Documente, gerencie e controle a integrida de das alteraçõe s em [Atribuição: itens de configura ção definidos pela organização sob gerenciamento de configuração]; (c) Implement e somente as alterações aprovadas pela organizaç ão no sistema, no componente ou no serviço; (d) Documente as alterações aprovadas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informaçõ es.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	A organização: (a) Implementa uma interface gerenciada para cada serviço externo de telecomunicações; (b) Estabelece uma política de fluxo de tráfego para cada interface gerenciada; (c) Protege a confidencialidade e a integridade das informações transmitidas por cada interface; (d) Documenta cada exceção à política de fluxo de tráfego com uma missão ou necessidade comercial de apoio e a duração dessa necessidade; e (e) Analisa as exceções à política de fluxo de tráfego [Atribuição: frequência definida pela organização] e remove exceções que não são mais compatíveis com uma missão ou necessidade de negócios	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	explícita. Orientaçã o complementar: Controle relacionado: SC-8.		
SC-7(5)	O sistema de informações em interfaces gerenciad as nega o tráfego de comunicaç ões de rede e permite o tráfego de comunicações de rede por exceção (ou seja, nega tudo, permite por exceção). Orientaçã o complementar: esse aprimoram ento de controle se aplica tanto ao tráfego de comunicações de rede de entrada quanto ao de saída. Uma política de negação de tráfego de comunicações de permit-by-exceptio n rede garante que somente as conexões essenciai s e aprovadas sejam permitidas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	O sistema de informações protege a confidencialidade e a integridade das informações transmitidas.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	O sistema de informações protege a confidencialidade E a integridade de [Atribuição: informações em repouso definidas pela organização].	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	A organização emprega mecanismos automatizados pelo menos uma vez ao mês para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	A organização emprega mecanismos automatizados pelo menos uma vez ao mês para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	A organização emprega mecanismos automatizados pelo menos uma vez ao mês para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	A organização emprega mecanismos automatizados pelo menos uma vez ao mês para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3	A organização: (a) Emprega mecanismos de proteção contra códigos mal-intencionados nos pontos de entrada e saída do sistema de informações para detectar e erradicar esses códigos; (b) Atualiza os mecanismos de proteção contra códigos mal-intencionados sempre que novas versões estão disponíveis, de acordo com a política e os procedimentos de gerenciamento de configuração organizacional; (c) Configura mecanismos de proteção contra códigos mal-intencionados para: 1. Realizar varreduras periódicas do sistema de informações [Atribuição: frequência definida pela organização] e varreduras em tempo real de	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	arquivos de fontes externas em [Seleção (uma ou mais): endpoint; pontos de entrada ou saída da rede] à medida que os arquivos são baixados, abertos ou executados de acordo com a política de segurança organizac ional; e 2. [Seleção (uma ou mais): bloquear códigos mal-intencionados; colocar códigos mal-intencionados em quarentena; enviar alerta ao administr ador; [Atribuição: ação definida pela organização]] em resposta à detecção de código mal-inten cionado; e (d) Aborda o recebimento de falsos positivos durante a detecção e a erradicação de códigos mal-inten cionados e o impacto potencial resultante na disponibilidade do sistema de informaçõ		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	es. Orientação complementar: os pontos de entrada e saída do sistema de informações incluem, por exemplo: firewalls, servidores de correio eletrônic o, servidores web, servidores proxy, servidores de acesso remoto, estações de trabalho, notebooks e dispositivos móveis. Um código mal-intencionado pode incluir vírus, worms, cavalos de Tróia e spyware. O código malicioso também pode ser codificado em vários formatos (por exemplo, UUENCODE, Unicode), contido em arquivos compactad os ou ocultos ou oculto em arquivos usando esteganog rafia. Ele pode ser transportado por diferentes meios, incluindo acessos à web, correio eletrônic		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	o, anexos de correio eletrônico e dispositivos de armazenamento portáteis. As inserções de código mal-intencionado ocorrem por meio da exploração de vulnerabilidades do sistema de informações. Os mecanismos de proteção contra códigos mal-intencionados incluem definições de assinatura de antivírus e tecnologias baseadas em reputação. Existem várias tecnologias e métodos para limitar ou eliminar os efeitos de códigos mal-intencionados. O amplo gerenciamento de configuração e os controles abrangentes de integridade do software podem ser eficazes na prevenção da execução de códigos não autorizados. Além do off-the-shelf		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	software comercial , códigos malicioso s também podem estar presentes em softwares personali zados. Isso abrange, por exemplo, bombas lógicas, backdoors e outros tipos de ataques cibernéti cos que podem impactar as missões ou funções comerciai s da organização. Os mecanismos tradicion ais de proteção contra códigos mal-intencionados nem sempre conseguem detectar esse código. Nessas situações, as organizações confiam em outras proteções , como práticas seguras de codificaç ão, gerenciamento e controle de configura ção, processos de aquisição confiáveis e práticas de monitoram ento para ajudar a garantir que o software não execute outras funções além		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	das pretendidas. As organizações podem determinar que, em resposta à detecção de código mal-intencionado, ações diferentes podem ser justifica das. Por exemplo, as organizações podem definir ações em resposta à detecção de códigos mal-intencionados durante verificações periódicas, ações em resposta à detecção de downloads mal-intencionados e/ou ações em resposta à detecção de códigos mal-intencionados ao tentar abrir ou executar arquivos. Controles relaciona dos: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referências: Publicação Especial 800-83 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3	A organização: (a) Emprega mecanismos de proteção contra códigos mal-intencionados nos pontos de entrada e saída do sistema de informações para detectar e erradicar esses códigos; (b) Atualiza os mecanismos de proteção contra códigos mal-intencionados sempre que novas versões estão disponíveis, de acordo com a política e os procedimentos de gerenciamento de configuração organizacional; (c) Configura mecanismos de proteção contra códigos mal-intencionados para: 1. Realizar varreduras periódicas do sistema de informações [Atribuição: frequência definida pela organização] e varreduras em tempo real de	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	arquivos de fontes externas em [Seleção (uma ou mais): endpoint; pontos de entrada ou saída da rede] à medida que os arquivos são baixados, abertos ou executados de acordo com a política de segurança organizac ional; e 2. [Seleção (uma ou mais): bloquear códigos mal-intencionados; colocar códigos mal-intencionados em quarentena; enviar alerta ao administr ador; [Atribuição: ação definida pela organização]] em resposta à detecção de código mal-inten cionado; e (d) Aborda o recebimento de falsos positivos durante a detecção e a erradicação de códigos mal-inten cionados e o impacto potencial resultante na disponibilidade do sistema de informaçõ		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	es. Orientação complementar: os pontos de entrada e saída do sistema de informações incluem, por exemplo: firewalls, servidores de correio eletrônic o, servidores web, servidores proxy, servidores de acesso remoto, estações de trabalho, notebooks e dispositivos móveis. Um código mal-intencionado pode incluir vírus, worms, cavalos de Tróia e spyware. O código malicioso também pode ser codificado em vários formatos (por exemplo, UUENCODE, Unicode), contido em arquivos compactad os ou ocultos ou oculto em arquivos usando esteganog rafia. Ele pode ser transportado por diferentes meios, incluindo acessos à web, correio eletrônic		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	o, anexos de correio eletrônico e dispositivos de armazenamento portáteis. As inserções de código mal-intencionado ocorrem por meio da exploração de vulnerabilidades do sistema de informações. Os mecanismos de proteção contra códigos mal-intencionados incluem definições de assinatura de antivírus e tecnologias baseadas em reputação. Existem várias tecnologias e métodos para limitar ou eliminar os efeitos de códigos mal-intencionados. O amplo gerenciamento de configuração e os controles abrangentes de integridade do software podem ser eficazes na prevenção da execução de códigos não autorizados. Além do off-the-shelf		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	software comercial , códigos malicioso s também podem estar presentes em softwares personali zados. Isso abrange, por exemplo, bombas lógicas, backdoors e outros tipos de ataques cibernéti cos que podem impactar as missões ou funções comerciai s da organização. Os mecanismos tradicion ais de proteção contra códigos mal-intencionados nem sempre conseguem detectar esse código. Nessas situações, as organizações confiam em outras proteções , como práticas seguras de codificaç ão, gerenciamento e controle de configura ção, processos de aquisição confiáveis e práticas de monitoram ento para ajudar a garantir que o software não execute outras funções além		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	das pretendidas. As organizações podem determinar que, em resposta à detecção de código mal-intencionado, ações diferentes podem ser justifica das. Por exemplo, as organizações podem definir ações em resposta à detecção de códigos mal-intencionados durante verificações periódicas, ações em resposta à detecção de downloads mal-intencionados e/ou ações em resposta à detecção de códigos mal-intencionados ao tentar abrir ou executar arquivos. Controles relaciona dos: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referências: Publicação Especial 800-83 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3	A organização: (a) Emprega mecanismos de proteção contra códigos mal-intencionados nos pontos de entrada e saída do sistema de informações para detectar e erradicar esses códigos; (b) Atualiza os mecanismos de proteção contra códigos mal-intencionados sempre que novas versões estão disponíveis, de acordo com a política e os procedimentos de gerenciamento de configuração organizacional; (c) Configura mecanismos de proteção contra códigos mal-intencionados para: 1. Realizar varreduras periódicas do sistema de informações [Atribuição: frequência definida pela organização] e varreduras em tempo real de	ecs-task-definition-memory-hard-limit	Limitar a memória máxima disponível para contêineres do Amazon Elastic Container Service (ECS) garante que não haja abuso no uso do recurso em caso de acesso mal-intencionado aos contêineres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	arquivos de fontes externas em [Seleção (uma ou mais): endpoint; pontos de entrada ou saída da rede] à medida que os arquivos são baixados, abertos ou executados de acordo com a política de segurança organizac ional; e 2. [Seleção (uma ou mais): bloquear códigos mal-intencionados; colocar códigos mal-intencionados em quarentena; enviar alerta ao administr ador; [Atribuição: ação definida pela organização]] em resposta à detecção de código mal-inten cionado; e (d) Aborda o recebimento de falsos positivos durante a detecção e a erradicação de códigos mal-inten cionados e o impacto potencial resultante na disponibilidade do sistema de informaçõ		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	es. Orientação complementar: os pontos de entrada e saída do sistema de informações incluem, por exemplo: firewalls, servidores de correio eletrônic o, servidores web, servidores proxy, servidores de acesso remoto, estações de trabalho, notebooks e dispositivos móveis. Um código mal-intencionado pode incluir vírus, worms, cavalos de Tróia e spyware. O código malicioso também pode ser codificado em vários formatos (por exemplo, UUENCODE, Unicode), contido em arquivos compactad os ou ocultos ou oculto em arquivos usando esteganog rafia. Ele pode ser transportado por diferentes meios, incluindo acessos à web, correio eletrônic		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	o, anexos de correio eletrônico e dispositivos de armazenamento portáteis. As inserções de código mal-intencionado ocorrem por meio da exploração de vulnerabilidades do sistema de informações. Os mecanismos de proteção contra códigos mal-intencionados incluem definições de assinatura de antivírus e tecnologias baseadas em reputação. Existem várias tecnologias e métodos para limitar ou eliminar os efeitos de códigos mal-intencionados. O amplo gerenciamento de configuração e os controles abrangentes de integridade do software podem ser eficazes na prevenção da execução de códigos não autorizados. Além do off-the-shelf		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	software comercial , códigos malicioso s também podem estar presentes em softwares personali zados. Isso abrange, por exemplo, bombas lógicas, backdoors e outros tipos de ataques cibernéti cos que podem impactar as missões ou funções comerciai s da organização. Os mecanismos tradicion ais de proteção contra códigos mal-intencionados nem sempre conseguem detectar esse código. Nessas situações, as organizações confiam em outras proteções , como práticas seguras de codificaç ão, gerenciamento e controle de configura ção, processos de aquisição confiáveis e práticas de monitoram ento para ajudar a garantir que o software não execute outras funções além		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	das pretendidas. As organizações podem determinar que, em resposta à detecção de código mal-intencionado, ações diferentes podem ser justifica das. Por exemplo, as organizações podem definir ações em resposta à detecção de códigos mal-intencionados durante verificações periódicas, ações em resposta à detecção de downloads mal-intencionados e/ou ações em resposta à detecção de códigos mal-intencionados ao tentar abrir ou executar arquivos. Controles relaciona dos: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7. Referências: Publicação Especial 800-83 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(1)	A organização conecta e configura ferramentas individuais de detecção de intrusões em um sistema de detecção de intrusões que abrange todo o sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferramentas automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferramentas automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
SI-4(2)	A organização emprega ferramentas automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	A organização emprega ferramentas automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(4)	O sistema de informações monitora continuamente o tráfego de comunicações de entrada e saída em busca de atividades ou condições incomuns ou não autorizadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(4)	O sistema de informações monitora continuamente o tráfego de comunicações de entrada e saída em busca de atividades ou condições incomuns ou não autorizadas.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(4)	O sistema de informações monitora continuamente o tráfego de comunicações de entrada e saída em busca de atividades ou condições incomuns ou não autorizadas.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(4)	O sistema de informações monitora continuamente o tráfego de comunicações de entrada e saída em busca de atividades ou condições incomuns ou não autorizadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicaçõe s de compromet imento ou possível comprometimento: [Atribuição: indicador es de compromet imento definidos pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicações de comprometimento ou possível comprometimento: [Atribuição: indicadores de comprometimento definidos pela organização].	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicaçõe s de compromet imento ou possível comprometimento: [Atribuição: indicador es de compromet imento definidos pela organização].	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicaçõe s de compromet imento ou possível comprometimento: [Atribuição: indicador es de compromet imento definidos pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	guardduty-non-arch ived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classific ando as descobert as por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégi as e prioridades de correção. Essa regra permite que você defina opcionalm ente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de transações de interesse para a organização.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	A organização: (a) Recebe alertas, recomendações e diretrizes de segurança do sistema de informações de [Atribuição: organizações externas definidas pela organização] de forma contínua; (b) Gera alertas, recomendações e diretrizes de segurança interna conforme necessário; (c) Divulga alertas, recomendações e diretrizes de segurança para: [Seleção (uma ou mais): [Atribuição: pessoal ou perfis definidos pela organização]; [Atribuição: elementos definidos pela organização dentro da organização]; [Atribuição: organizações externas definidas pela organização]]; e (d) Implement a diretrizes de	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	segurança de acordo com prazos estabelecidos ou notifica a organização emissora sobre o grau de não conformidade. Orientação complementar: a US-CERT (The United States Computer Emergency Readiness Team) gera alertas e recomendações de segurança para manter a consciência situacional em todo o governo federal. As diretivas de segurança são emitidas pelo OMB (Office of Management and Budget) ou por outras organizações designadas com a responsabilidade e autoridade para emitir tais diretivas. A conformidade com as diretivas de segurança é essencial devido à natureza essencial de muitas dessas diretivas e		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	aos potenciais efeitos adversos imediatos nas operações e nos ativos organizac ionais, nos indivíduos, em outras organizaç ões e na nação, caso as diretivas não sejam implement adas em tempo hábil. As organizações externas incluem, por exemplo, parceiros externos de missão e negócios, parceiros da cadeia de suprimentos, prestadores de serviços externos e outras organizações de parceiros ou apoio. Controle relaciona do: SI-2. Referências: Publicação Especial 800-40 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	A organização: (a) Recebe alertas, recomendações e diretrizes de segurança do sistema de informações de [Atribuição: organizações externas definidas pela organização] de forma contínua; (b) Gera alertas, recomendações e diretrizes de segurança interna conforme necessário; (c) Divulga alertas, recomendações e diretrizes de segurança para: [Seleção (uma ou mais): [Atribuição: pessoal ou perfis definidos pela organização]; [Atribuição: elementos definidos pela organização dentro da organização]; [Atribuição: organizações externas definidas pela organização]]; e (d) Implement a diretrizes de	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	segurança de acordo com prazos estabelecidos ou notifica a organização emissora sobre o grau de não conformidade. Orientação complementar: a US-CERT (The United States Computer Emergency Readiness Team) gera alertas e recomendações de segurança para manter a consciência situacional em todo o governo federal. As diretivas de segurança são emitidas pelo OMB (Office of Management and Budget) ou por outras organizações designadas com a responsabilidade e autoridade para emitir tais diretivas. A conformidade com as diretivas de segurança é essencial devido à natureza essencial de muitas dessas diretivas e		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	aos potenciais efeitos adversos imediatos nas operações e nos ativos organizac ionais, nos indivíduos, em outras organizaç ões e na nação, caso as diretivas não sejam implement adas em tempo hábil. As organizações externas incluem, por exemplo, parceiros externos de missão e negócios, parceiros da cadeia de suprimentos, prestadores de serviços externos e outras organizações de parceiros ou apoio. Controle relaciona do: SI-2. Referências: Publicação Especial 800-40 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	A organização: (a) Recebe alertas, recomendações e diretrizes de segurança do sistema de informações de [Atribuição: organizações externas definidas pela organização] de forma contínua; (b) Gera alertas, recomendações e diretrizes de segurança interna conforme necessário; (c) Divulga alertas, recomendações e diretrizes de segurança para: [Seleção (uma ou mais): [Atribuição: pessoal ou perfis definidos pela organização]; [Atribuição: elementos definidos pela organização dentro da organização]; [Atribuição: organizações externas definidas pela organização]]; e (d) Implement a diretrizes de	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	segurança de acordo com prazos estabelecidos ou notifica a organização emissora sobre o grau de não conformidade. Orientação complementar: a US-CERT (The United States Computer Emergency Readiness Team) gera alertas e recomendações de segurança para manter a consciência situacional em todo o governo federal. As diretivas de segurança são emitidas pelo OMB (Office of Management and Budget) ou por outras organizações designadas com a responsabilidade e autoridade para emitir tais diretivas. A conformidade com as diretivas de segurança é essencial devido à natureza essencial de muitas dessas diretivas e		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	aos potenciais efeitos adversos imediatos nas operações e nos ativos organizac ionais, nos indivíduos, em outras organizaç ões e na nação, caso as diretivas não sejam implement adas em tempo hábil. As organizações externas incluem, por exemplo, parceiros externos de missão e negócios, parceiros da cadeia de suprimentos, prestadores de serviços externos e outras organizações de parceiros ou apoio. Controle relaciona do: SI-2. Referências: Publicação Especial 800-40 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-5	A organização: (a) Recebe alertas, recomendações e diretrizes de segurança do sistema de informações de [Atribuição: organizações externas definidas pela organização] de forma contínua; (b) Gera alertas, recomendações e diretrizes de segurança interna conforme necessário; (c) Divulga alertas, recomendações e diretrizes de segurança para: [Seleção (uma ou mais): [Atribuição: pessoal ou perfis definidos pela organização]; [Atribuição: elementos definidos pela organização dentro da organização]; [Atribuição: organizações externas definidas pela organização]]; e (d) Implement a diretrizes de	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	segurança de acordo com prazos estabelecidos ou notifica a organização emissora sobre o grau de não conformidade. Orientação complementar: a US-CERT (The United States Computer Emergency Readiness Team) gera alertas e recomendações de segurança para manter a consciência situacional em todo o governo federal. As diretivas de segurança são emitidas pelo OMB (Office of Management and Budget) ou por outras organizações designadas com a responsabilidade e autoridade para emitir tais diretivas. A conformidade com as diretivas de segurança é essencial devido à natureza essencial de muitas dessas diretivas e		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	aos potenciais efeitos adversos imediatos nas operações e nos ativos organizac ionais, nos indivíduos, em outras organizaç ões e na nação, caso as diretivas não sejam implement adas em tempo hábil. As organizações externas incluem, por exemplo, parceiros externos de missão e negócios, parceiros da cadeia de suprimentos, prestadores de serviços externos e outras organizações de parceiros ou apoio. Controle relaciona do: SI-2. Referências: Publicação Especial 800-40 do NIST.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(1)	O sistema de informações realiza uma verificação de integridade de eventos relevante s à segurança pelo menos uma vez por mês.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(1)	O sistema de informações realiza uma verificação de integridade de eventos relevantes à segurança pelo menos uma vez por mês.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(1)	O sistema de informações realiza uma verificação de integridade de eventos relevante s à segurança pelo menos uma vez por mês.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7	A organização emprega ferrament as de verificação de integridade para detectar alterações não autorizadas em [Atribuição: softwares, firmwares e informaçõ es definidos pela organização].	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatc h ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informaçõ es detalhadas sobre o projeto de compilaçã o.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-11	O sistema de informações: (a) Gera mensagens de erro que fornecem as informações necessárias para realizar ações corretivas sem revelar informaçõ es que poderiam ser exploradas por invasores; e (b) Revela mensagens de erro somente para [Atribuição: pessoal ou funções definidas pela organizaç ão]. Orientaçã o complemen tar: as organizaç ões consideram cuidadosamente a estrutura e o conteúdo das mensagens de erro. O alcance que os sistemas de informações são capazes de identificar e lidar com condições de erro é orientado pela política organizac ional e pelos requisito	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s operacionais. As informações que podem ser exploradas por invasores incluem tentativas errôneas de login com senhas inseridas por engano no campo do nome de usuário, informaçõ es comerciais ou da missão que podem ser derivadas (se não declaradas explicita mente) das informaçõ es registradas e informações pessoais, como números de contas, CPF e números de cartão de crédito. Além disso, as mensagens de erro podem fornecer um canal secreto para transmiti r informações. Controles relaciona dos: AU-2, AU-3, SC-31. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-16	O sistema de informações implementa [Atribuição: proteções de segurança definidas pela organização] para proteger sua memória da execução não autorizada de código. Orientação complementar: alguns invasores realizam ataques com a intenção de executar código em regiões não executáveis da memória ou em locais de memória proibidos. As proteções de segurança empregadas para proteger a memória incluem a prevenção da execução de dados e a randomização do layout do espaço de endereço. As proteções de prevenção de execução de dados podem ser aplicadas por hardware ou por software, com o	ecs-task-definition-memory-hard-limit	Limitar a memória máxima disponível para contêineres do Amazon Elastic Container Service (ECS) garante que não haja abuso no uso do recurso em caso de acesso mal-intencionado aos contêineres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	hardware fornecend o a maior força dex mecanismo. Controles relacionados: AC-25, SC-3. Aprimoram entos de controle: nenhum. Referências: nenhuma.		

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o FedRAMP (moderado).

Operational Best Practices for FFIEC

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os domínios da Ferramenta de Avaliação de Segurança Cibernética do Federal Financial Institutions Examination Council (FFIEC) e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles da Ferramenta de Avaliação de Segurança Cibernética da FFIEC. O controle da Ferramenta de Avaliação de Segurança Cibernética da FFIEC pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.G.IT.B.1	Um inventário de ativos organizac ionais (por exemplo, hardware, software, dados e sistemas hospedados externamente) é mantido.	ec2-instance-manag ed-by-systems-mana ger	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
D1.G.IT.B.1	Um inventário de ativos organizac ionais (por exemplo, hardware, software, dados e sistemas hospedados	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2)

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	externamente) é mantido.		verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
D1.G.IT.B.1	Um inventário de ativos organizacionais (por exemplo, hardware, software, dados e sistemas hospedados externamente) é mantido.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.G.IT.B.1	Um inventário de ativos organizac ionais (por exemplo, hardware, software, dados e sistemas hospedados externamente) é mantido.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.Rm.B.1	Há algumas funções de gerenciamento de riscos de segurança da informação e continuidade de negócios dentro da instituição.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.RM.RA.B.2	A avaliação de risco identifica sistemas baseados na Internet e transações de alto risco que garantem controles adicionais de autenticação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
D1.RM.RA.B.2	A avaliação de risco identifica sistemas baseados na Internet e transações de alto risco que garantem controles adicionais de autenticação.	annual-risk-assess ment-performed (verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabili dade e o impacto dos riscos e/ou vulnerabi lidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.TC.Tr.B.2	O treinamento anual em segurança da informação inclui resposta a incidentes, ameaças cibernéticas atuais (por exemplo, phishing, spear phishing, engenhari a social e segurança móvel) e questões emergentes.	security-awareness -program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
D2.IS.Is.B.1	As ameaças à segurança da informação são coletadas e compartil hadas com os funcionários internos aplicáveis.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.IS.Is.B.1	As ameaças à segurança da informação são coletadas e compartilhadas com os funcionários internos aplicáveis.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.IS.Is.B.1	As ameaças à segurança da informação são coletadas e compartil hadas com os funcionários internos aplicáveis.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
D2.MA.Ma.B.1	Os registros de auditoria e outros registros de eventos de segurança são revisados e retidos de forma segura.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.MA.Ma.B.2	Os registros de eventos do computador são usados para investigações após a ocorrência de um evento.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.1	A instituição pertence ou assina uma fonte de compartilhamento de informações sobre ameaças e vulnerabilidades que fornece informações sobre ameaças (por exemplo, FS-ISAC, US-CERT).	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.1	A instituição pertence ou assina uma fonte de compartilhamento de informações sobre ameaças e vulnerabilidades que fornece informações sobre ameaças (por exemplo, FS-ISAC, US-CERT).	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.2	As informações sobre ameaças são usadas para monitorar ameaças e vulnerabilidades.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.2	As informações sobre ameaças são usadas para monitorar ameaças e vulnerabilidades.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.2	As informações sobre ameaças são usadas para monitorar ameaças e vulnerabilidades.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.3	As informações sobre ameaças são usadas para aprimorar o gerenciamento e os controles internos de riscos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D2.TI.Ti.B.3	As informações sobre ameaças são usadas para aprimorar o gerenciamento e os controles internos de riscos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.1	Um programa de gerenciamento de patches é implement ado e garante que os patches de software e firmware sejam aplicados em tempo hábil.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.1	Um programa de gerenciamento de patches é implemented e garante que os patches de software e firmware sejam aplicados em tempo hábil.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.1	Um programa de gerenciamento de patches é implemented e garante que os patches de software e firmware sejam aplicados em tempo hábil.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.1	Um programa de gerenciamento de patches é implementado e garante que os patches de software e firmware sejam aplicados em tempo hábil.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.3	Os relatórios de gerenciamento de patches são revisados e refletem os patches de segurança ausentes.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.3	Os relatórios de gerenciamento de patches são revisados e refletem os patches de segurança ausentes.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.3	Os relatórios de gerenciamento de patches são revisados e refletem os patches de segurança ausentes.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.CC.PM.B.3	Os relatórios de gerenciamento de patches são revisados e refletem os patches de segurança ausentes.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.1	A instituição é capaz de detectar atividades anômalas por meio do monitoramento em todo o ambiente.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.1	A instituição é capaz de detectar atividades anômalas por meio do monitoramento em todo o ambiente.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.1	A instituição é capaz de detectar atividades anômalas por meio do monitoramento em todo o ambiente.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.2	As transações dos clientes que geram alertas de atividades anômalas são monitoradas e revisadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.2	As transações dos clientes que geram alertas de atividades anômalas são monitoradas e revisadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.3	Os registros de acesso físico e/ou lógico são revisados após os eventos.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
D3.DC.An.B.4	O acesso a sistemas críticos por terceiros é monitorado em busca de atividades não autorizadas ou incomuns	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.An.B.5	Privilégios elevados são monitorados.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
D3.DC.An.B.5	Privilégios elevados são monitorados.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelec ida.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelec ida.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelecida.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.1	Uma linha de base normal da atividade da rede é estabelec ida.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.2	Mecanismos (por exemplo, alertas de antivírus, alertas de eventos de log) existem para alertar o gerenciamento sobre possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.3	Existem processos para monitorar a presença de usuários, dispositivos, conexões e software não autorizados.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.3	Existem processos para monitorar a presença de usuários, dispositivos, conexões e software não autorizados.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.3	Existem processos para monitorar a presença de usuários, dispositivos, conexões e software não autorizados.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Ev.B.3	Existem processos para monitorar a presença de usuários, dispositivos, conexões e software não autorizados.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Th.B.1	Testes independentes (incluindo testes de penetração e verificação de vulnerabilidades) são conduzidos de acordo com a avaliação de risco de sistemas externos e da rede interna.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Th.B.1	Testes independentes (incluindo testes de penetração e verificação de vulnerabilidades) são conduzidos de acordo com a avaliação de risco de sistemas externos e da rede interna.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.DC.Th.B.1	Testes independentes (incluindo testes de penetração e verificação de vulnerabilidades) são conduzidos de acordo com a avaliação de risco de sistemas externos e da rede interna.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenciais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenciais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenc iais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
D3.PC.Am.B.1	O acesso dos funcionários é concedido a sistemas e dados confidenciais com base nas responsabilidades do trabalho e nos princípios de privilégio mínimo.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.10	Os ambientes de produção e não produção são separados para evitar acesso não autorizado ou alterações nos ativos de informações. (*N/A se não existir ambiente de produção na instituição ou em terceiros da instituição.)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.10	Os ambientes de produção e não produção são separados para evitar acesso não autorizado ou alterações nos ativos de informações. (*N/A se não existir ambiente de produção na instituição ou em terceiros da instituição.)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.10	Os ambientes de produção e não produção são separados para evitar acesso não autorizado ou alterações nos ativos de informações. (*N/A se não existir ambiente de produção na instituição ou em terceiros da instituição.)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.10	Os ambientes de produção e não produção são separados para evitar acesso não autorizado ou alterações nos ativos de informações. (*N/A se não existir ambiente de produção na instituição ou em terceiros da instituição.)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administr ativas sobre cada entidade principal.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
D3.PC.Am.B.12	Todas as senhas são criptografadas no armazenamento e em trânsito.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.13	Os dados confidenciais são criptografados quando transmitidos por redes públicas ou não confiáveis (por exemplo, Internet).	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifato rial.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.15	O acesso remoto a sistemas críticos por funcionários, prestadores de serviços e terceiros usa conexões criptografadas e autenticação multifatorial.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.16	Existem controles administrativos, físicos ou técnicos para impedir que usuários sem responsabilidades administrativas instalem software não autorizado.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.16	Existem controles administrativos, físicos ou técnicos para impedir que usuários sem responsabilidades administrativas instalem software não autorizado.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.16	Existem controles administrativos, físicos ou técnicos para impedir que usuários sem responsabilidades administrativas instalem software não autorizado.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
D3.PC.Am.B.16	Existem controles administrativos, físicos ou técnicos para impedir que usuários sem responsabilidades administrativas instalem software não autorizado.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.2	O acesso dos funcionários aos sistemas e dados confidenciais permite a separação de deveres.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.2	O acesso dos funcionários aos sistemas e dados confidenciais permite a separação de deveres.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
D3.PC.Am.B.2	O acesso dos funcionários aos sistemas e dados confidenciais permite a separação de deveres.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes).	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes)	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.3	Privilégios elevados (por exemplo, privilégios de administrador) são limitados e rigidamente controlados (por exemplo, atribuídos a indivíduos, não compartilhados e exigem controles de senha mais fortes)	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessári as e gerenciad as para acesso a sistemas, aplicações e hardware.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessári as e gerenciad as para acesso a sistemas, aplicações e hardware.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessári as e gerenciad as para acesso a sistemas, aplicações e hardware.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessárias e gerenciadas para acesso a sistemas, aplicações e hardware.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.6	A identificação e a autenticação são necessári as e gerenciad as para acesso a sistemas, aplicações e hardware.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
D3.PC.Am.B.6	A identificação e a autenticação são necessári as e gerenciad as para acesso a sistemas, aplicações e hardware.	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.7	Os controles de acesso incluem complexidade da senha, limites para uso de senha incorreta e reutilização de senhas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Am.B.8	Todas as senhas e contas padrão desnecessárias são alteradas antes da implementação do sistema.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.1	Ferramentas de defesa do perímetro de rede (por exemplo, roteador de fronteira e firewall) são usadas.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.2	Os sistemas acessados pela Internet ou por terceiros são protegidos por firewalls ou outros dispositivos semelhantes.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.3	Todas as portas são monitoradas.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
D3.PC.IM.B.3	Todas as portas são monitoradas.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.3	Todas as portas são monitoradas.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.3	Todas as portas são monitoradas.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.3	Todas as portas são monitoradas.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.3	Todas as portas são monitoradas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.5	As configurações de sistemas (para servidores, desktops, roteadores etc.) seguem os padrões do setor e são aplicadas	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.5	As configurações de sistemas (para servidores, desktops, roteadores etc.) seguem os padrões do setor e são aplicadas	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.5	As configurações de sistemas (para servidores, desktops, roteadores etc.) seguem os padrões do setor e são aplicadas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.6	Portas, funções, protocolos e serviços serão proibidos se não forem mais necessários para fins comerciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.6	Portas, funções, protocolos e serviços serão proibidos se não forem mais necessários para fins comerciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.6	Portas, funções, protocolos e serviços serão proibidos se não forem mais necessários para fins comerciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.IM.B.6	Portas, funções, protocolos e serviços serão proibidos se não forem mais necessários para fins comerciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alteraçõe s nas configura ções do sistema (incluindo máquinas virtuais e hiperviso res) é controlado e monitorado.	iam-user-group-mem bership-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantind o que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alteraçõe s nas configura ções do sistema (incluindo máquinas virtuais e hiperviso res) é controlado e monitorado.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alteraçõe s nas configura ções do sistema (incluindo máquinas virtuais e hiperviso res) é controlado e monitorado.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alterações nas configurações do sistema (incluindo máquinas virtuais e hipervisores) é controlado e monitorado.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alteraçõe s nas configura ções do sistema (incluindo máquinas virtuais e hiperviso res) é controlado e monitorado.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
D3.PC.Im.B.7	O acesso para fazer alteraçõe s nas configura ções do sistema (incluindo máquinas virtuais e hiperviso res) é controlado e monitorado.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Im.B.7	O acesso para fazer alterações nas configurações do sistema (incluindo máquinas virtuais e hipervisores) é controlado e monitorado.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Se.B.1	Os desenvolvedores que trabalham para a instituição seguem práticas seguras de codificação de programas, como parte de um ciclo de vida de desenvolvimento do sistema (SDLC), que atende aos padrões do setor.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D3.PC.Se.B.1	Os desenvolvedores que trabalham para a instituição seguem práticas seguras de codificação de programas, como parte de um ciclo de vida de desenvolv imento do sistema (SDLC), que atende aos padrões do setor.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D4.C.Co.B.2	A instituição garante que as conexões de terceiros sejam autorizadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D4.C.Co.B.2	A instituição garante que as conexões de terceiros sejam autorizadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D4.C.Co.B.2	A instituição garante que as conexões de terceiros sejam autorizadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D4.C.Co.B.2	A instituição garante que as conexões de terceiros sejam autorizadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.1	Os parâmetros de alerta são definidos para detectar incidentes de segurança da informação que estimulam ações mitigadoras.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.1	Os parâmetros de alerta são definidos para detectar incidentes de segurança da informação que estimulam ações mitigadoras.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.1	Os parâmetros de alerta são definidos para detectar incidentes de segurança da informação que estimulam ações mitigadoras.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
D5.DR.De.B.2	Os relatórios de desempenho do sistema contêm informações que podem ser usadas como um indicador de risco para detectar incidentes contra a segurança da informação	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.2	Os relatórios de desempenho do sistema contêm informações que podem ser usadas como um indicador de risco para detectar incidentes contra a segurança da informação	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
D5.DR.De.B.3	Existem ferrament as e processos para detectar, alertar e acionar o programa de resposta a incidentes.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.DR.De.B.3	Existem ferramentas e processos para detectar, alertar e acionar o programa de resposta a incidentes.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.ER.Es.B.4	Os incidentes são classificados, registrados e rastreados.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.
D5.IR.Pl.B.1	A instituição documentou como reagirá e responderá aos incidentes cibernéticos.	response-plan-exists-maintained (verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperaç ão de desastres e backup de dados para recuperar as operações após um incidente.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperaç ão de desastres e backup de dados para recuperar as operações após um incidente.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D5.IR.PI.B.6	A instituição planeja usar programas de continuidade de negócios, recuperação de desastres e backup de dados para recuperar as operações após um incidente.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o FFIEC.

Práticas recomendadas operacionais do Catálogo de Critérios de Conformidade de Computação em Nuvem da Alemanha (C5)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Catálogo de Critérios de Conformidade de Computação em Nuvem (C5) da Alemanha e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles C5 da Alemanha. Um controle do C5 da Alemanha pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
COS-01	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
COS-01	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você

ID de controle	AWS Regra de configuração	Orientação
		define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
COS-01	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
COS-01	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencion al.
COS-01	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	AWS Regra de configuração	Orientação
COS-01	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
COS-03	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
COS-03	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
COS-03	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
COS-03	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
COS-03	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
COS-03	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
COS-03	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
COS-03	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
COS-03	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectado s somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
COS-03	lambda-function-public-acce ss-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
COS-03	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
COS-03	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
COS-03	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
COS-03	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
COS-03	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
COS-03	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
COS-03	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
COS-03	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
COS-03	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
COS-03	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
COS-03	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
COS-05	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
COS-05	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
COS-05	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
COS-05	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
COS-05	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
COS-05	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
COS-05	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
COS-05	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
COS-05	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
COS-05	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
COS-05	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
COS-05	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
COS-05	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
CRY-02	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CRY-02	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
CRY-02	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefini das usadas para a negociaçã o SSL quando é estabelec ida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográ ficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptore s SSL. A política de segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
CRY-02	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
CRY-02	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
CRY-02	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
CRY-02	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CRY-02	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CRY-02	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
CRY-03	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
CRY-03	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
CRY-03	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Kinesis Streams.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
CRY-03	dynamodb-table-encrypted-km s	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
CRY-03	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
CRY-03	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
CRY-03	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
CRY-03	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
CRY-03	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
CRY-03	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
CRY-03	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
CRY-03	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
CRY-03	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
CRY-03	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
CRY-04	cmk-backing-key-rotation-en abled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográ fico.
DEV-07	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
DEV-07	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
DEV-07	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
DEV-07	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
DEV-07	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	AWS Regra de configuração	Orientação
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IDM-01	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
IDM-01	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
IDM-01	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
IDM-01	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
IDM-01	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
IDM-01	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programaç ão regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
IDM-01	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
IDM-01	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	ecs-containers-nonprivileged	Para ajudar na implement ação do princípio de privilégi o mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégi o elevado habilitado. Quando esse parâmetro é verdadeir o, o contêiner recebe privilégi os elevados na instância de contêiner host (semelhante ao usuário raiz).
IDM-01	ecs-containers-readonly-acc ess	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
IDM-01	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	efs-access-point-enforce-user-identity	Para ajudar na implement ação do princípio de privilégi o mínimo, habilite a fiscaliza ção do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configura da no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.
IDM-01	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
IDM-01	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
IDM-01	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente.
IDM-01	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	AWS Regra de configuração	Orientação
IDM-03	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
IDM-03	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credencia is, pois isso pode violar o princípio do menor privilégi o. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
IDM-08	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
CHOR-01	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
IDM-09	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
IDM-09	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
IDM-09	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
IDM-09	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
OPS-01	clb-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêiner es e endereços IP, em uma ou mais zonas de disponibi lidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	AWS Regra de configuração	Orientação
OPS-01	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêiner es e endereços IP, em uma ou mais zonas de disponibi lidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.
OPS-01	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibilidade diferentes para garantir que sua função esteja disponíve l para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	AWS Regra de configuração	Orientação
OPS-01	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitad a para auxiliar na disponibi lidade dos dados armazenad os. Cada zona de disponibi lidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
OPS-01	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
OPS-01	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
OPS-01	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
OPS-01	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	clb-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêiner es e endereços IP, em uma ou mais zonas de disponibi lidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.
OPS-02	autoscaling-group-elb-healt hcheck-required	As verificações de integrida de do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutençã o de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instância s do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
OPS-02	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibilidade diferentes para garantir que sua função esteja disponíve l para processar eventos em caso de interrupção do serviço em uma única zona.
OPS-02	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitad a para auxiliar na disponibi lidade dos dados armazenad os. Cada zona de disponibi lidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
OPS-02	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
OPS-02	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
OPS-07	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
OPS-07	opensearch-data-node-fault-tolerance	O Amazon OpenSearch Service (OpenSearch Service) exige pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um domínio OpenSearch de serviço com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
OPS-07	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
OPS-07	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
OPS-07	elasticache-redis-cluster-automatic-backup-check	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
OPS-07	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
OPS-07	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
OPS-12	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
OPS-12	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenam ento, arquivá-los ou excluí-lo s após um período especific ado).
OPS-13	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
OPS-13	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
OPS-13	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
OPS-14	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
OPS-14	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
OPS-14	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.
OPS-14	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenam ento, arquivá-los ou excluí-lo s após um período especific ado).
OPS-15	api-gw-execution-logging-en abled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
OPS-15	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
OPS-15	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
OPS-15	opensearch-audit-logging-en abled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
OPS-15	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
OPS-15	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
OPS-15	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
OPS-15	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
OPS-15	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
OPS-15	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
OPS-22	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.
PSS-05	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
PSS-05	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
PSS-05	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
PSS-05	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
PSS-07	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

Modelo

O modelo está disponível em GitHub: Catálogo de critérios de conformidade de computação em nuvem da Alemanha (C5).

Práticas recomendadas operacionais para o Gramm Leach Bliley Act (GLBA)

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja abaixo um exemplo de mapeamento entre a Lei Gramm-Leach-Bliley (GLBA) e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles GLBA. Um controle da GLBA pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas		replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	autoscaling-launch-config-public-ip-disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	dynamodb-table-encrypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenad os no Amazon S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(1)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (1) para garantir a segurança e confidencialidade dos registros e informaçõ es do cliente;	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(2)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (2) para proteger contra ameaças ou riscos previstos à segurança ou integridade desses registros; e	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(2)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (2) para proteger contra ameaças ou riscos previstos à segurança ou integridade desses registros; e	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	secretsmanager-rot ation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-policy-no-stat ements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-user-group-membership-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a restringir permissõe s e autorizações de acesso, garantind o que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguardas administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizado desses registros ou informações que poderia resultar em danos ou inconveniência significativos para qualquer cliente.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	s3-bucket-policy-g rantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_po licy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados , entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	ecs-containers-rea donly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégi o mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	efs-access-point-e nforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringi r o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especific ado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
GLBA-SEC.501(b)(3)	No cumprimento da política na subseção (a), cada agência ou autoridade descrita na seção 505 (a) deverá estabelecer padrões apropriados para as instituições financeiras sujeitas à sua jurisdição em relação a salvaguar das administrativas, técnicas e físicas (3) para proteger contra acesso ou uso não autorizad o desses registros ou informações que poderia resultar em danos ou inconveni ência significativos para qualquer cliente.	efs-access-point-e nforce-user-identity	Para ajudar na implementação do princípio de privilégi o mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configura da no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para a Lei Gramm Leach Bliley (GLBA).

Práticas recomendadas operacionais para o Anexo 11 da GxP da UE

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir

totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Anexo 11 da GxP EU e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles GxP EU Anexo 11. Um controle do Anexo 11 da GxP da UE pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Gestão de riscos	A gestão de riscos deve ser aplicada em todo o ciclo de vida do sistema informati zado, considera ndo a segurança do paciente, a integrida de dos dados e a qualidade do produto. Como parte de um sistema de gestão de riscos, as decisões sobre a extensão dos controles de validação e integrida de dos dados devem ser baseadas em uma avaliação de risco justificada e documentada do sistema informati zado.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Gestão de riscos	A gestão de riscos deve ser aplicada em todo o ciclo de vida do sistema informati zado, considera ndo a segurança do paciente, a integrida de dos dados e a qualidade do produto. Como parte de um sistema de gestão de riscos, as decisões sobre a extensão dos controles de validação e integrida de dos dados devem ser baseadas em uma avaliação de risco justificada e documentada do sistema informati zado.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.2. Validação - Controle de Alterações na Documentação	A documentação de validação deve incluir registros de controle das alterações (se aplicável) e relatórios sobre desvios observados durante o processo de validação.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponível. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhando os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponível. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhando os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponível. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhando os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	ec2-security-group-attached-to-eni-periodic	Para ajudar a gerenciar seu inventário de ativos, essa regra verifica se grupos de segurança estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma interface de rede elástica. Se os grupos de segurança não estiverem vinculados a esses tipos de recursos, eles podem não ser usados e não serem mais necessários.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponíve l. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhand o os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponíve l. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhand o os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.3. Validação - Inventário	Uma lista atualizada de todos os sistemas relevantes e suas funcionalidades de GMP (inventário) deve estar disponível. Para sistemas críticos, é preciso disponibilizar uma descrição atualizada do sistema detalhando os arranjos físicos e lógicos, fluxos de dados e interfaces com outros sistemas ou processos, pré-requisitos de hardware e software e medidas de segurança.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significado dos dados não sejam alterados durante o processo de migração.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.8. Validação - Transferência de dados	Se os dados forem transferidos para outro formato de dados ou sistema, a validação deverá incluir verificações para garantir que o valor e/ou significa do dos dados não sejam alterados durante o processo de migração.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informati zados que trocam dados eletronic amente com outros sistemas devem incluir verificações integradas apropriad as para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informatizados que trocam dados eletronicamente com outros sistemas devem incluir verificações integradas apropriadas para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Dados	Os sistemas informati zados que trocam dados eletronic amente com outros sistemas devem incluir verificações integradas apropriad as para a entrada e o processamento corretos e seguros dos dados, a fim de minimizar os riscos.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	dynamodb-table-enc rypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônicos contra danos. Os dados armazenados devem ser verificados quanto à acessibilidade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1. Armazenamento de dados - Proteção contra danos	Os dados devem ser protegidos por meios físicos e eletrônic os contra danos. Os dados armazenados devem ser verificad os quanto à acessibil idade, legibilidade e precisão. O acesso aos dados deve ser garantido durante todo o período de retenção.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	aurora-resources-p rotected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	backup-plan-min-fr equency-and-min-re tention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyV alue parâmetros (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredF requencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	ebs-optimized-inst ance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimizaçã o proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	ebs-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	ec2-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	efs-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	fsx-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2. Armazenamento de dados - Backups	É preciso fazer backups regulares de todos os dados relevantes. A integrida de e a precisão dos dados de backup e a capacidade de restaurá-los devem ser verificadas durante a validação e monitoradas periodica mente.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Trilhas de auditoria	Com base em uma avaliação de risco, considere incorporar ao sistema a criação de um registro de todas as alterações e exclusões relevantes ao GMP (uma “trilha de auditoria” gerada pelo sistema). Para alteração ou exclusão de dados relevante s ao GMP, o motivo deve ser documenta do. As trilhas de auditoria precisam estar disponíve is e ser conversív eis em um formato geralmente inteligível e revisadas regularme nte.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Gerenciamento de alterações e configurações	Alterações em um sistema informatizado, incluindo configurações do sistema, só devem ser feitas de forma controlada, seguindo um procedimento definido.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
10. Gerenciamento de alterações e configurações	Alterações em um sistema informatizado, incluindo configurações do sistema, só devem ser feitas de forma controlada, seguindo um procedimento definido.	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Gerenciamento de alterações e configurações	Alterações em um sistema informatizado, incluindo configurações do sistema, só devem ser feitas de forma controlada, seguindo um procedimento definido.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Período de avaliação	Os sistemas computadorizados devem ser avaliados periodicamente para confirmar que permanecem em um estado válido e estão em conformidade com o GMP. Essas avaliações devem incluir, quando apropriado, as opções atuais de funcionalidades, registros de desvios, incidentes, problemas, histórico de atualizações, relatórios de desempenho, confiabilidade, segurança e status de validação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.1. Segurança - Pessoas autorizadas	É necessário haver controles físicos e/ou lógicos para restringir o acesso do sistema computadorizado às pessoas autorizadas. Os métodos adequados para impedir a entrada não autorizada no sistema podem incluir o uso de chaves, cartões de acesso, códigos pessoais com senhas, biometria, acesso restrito a equipamentos de informática e áreas de armazenamento de dados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.3. Segurança - Trilha de auditoria de autorização	A criação, alteração e cancelamento das autorizações de acesso devem ser registrados.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetado s para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12.4. Segurança - Trilha de auditoria	Os sistemas de gerenciamento de dados e documentos devem ser projetados para registrar a identidade dos operadores que inserem, alteram, confirmam ou excluem dados, incluindo data e hora.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13. Gerenciamento de incidentes	Todos os incidente s, não apenas falhas do sistema e erros de dados, devem ser relatados e avaliados . A causa raiz de um incidente crítico deve ser identificada e formar a base das ações corretivas e preventivas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13. Gerenciamento de incidentes	Todos os incidente s, não apenas falhas do sistema e erros de dados, devem ser relatados e avaliados . A causa raiz de um incidente crítico deve ser identificada e formar a base das ações corretivas e preventivas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibilidade diferentes para garantir que sua função esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	opensearch-data-node-fault-tolerance	O Amazon OpenSearch Service (OpenSearch Service) exige pelo menos três nós de dados para alta disponibilidade e tolerância a falhas. A implantação de um domínio OpenSearch de serviço com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informatizados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternativos em uso deve ser baseado no risco e ser adequado a um sistema específico e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitada para auxiliar na disponibilidade dos dados armazenados. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
16. Continuidade dos negócios	Para a disponibilidade de sistemas informati zados que suportem processos críticos, devem ser tomadas medidas para garantir a continuidade do suporte a esses processos em caso de avaria do sistema (por exemplo, um sistema manual ou alternativo). O tempo necessário para colocar esses processos alternati vos em uso deve ser baseado no risco e ser adequado a um sistema específic o e ao processo de negócios que ele suporta. Esses processos devem ser adequadamente documentados e testados.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
17. Arquivamento	Os dados podem ser arquivados. Os dados devem ser verificados quanto à acessibilidade, legibilidade e precisão. Se mudanças relevantes precisarem ser feitas no sistema (por exemplo, equipamentos ou programas de computador), a capacidade de recuperar os dados deve ser garantida e testada.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

Modelo

O modelo está disponível em GitHub: Boas práticas operacionais para a GxP EU, Anexo 11.

Operational Best Practices for HIPAA Security

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é

responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles HIPAA. Um controle da HIPAA pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse pacote de conformidade foi validado pela AWS Security Assurance Services LLC (AWS SAS), que é uma equipe de avaliadores de segurança qualificados do setor de cartões de pagamento (QSAs), profissionais certificados pela HITRUST Common Security Framework (CCSFPs) e profissionais de conformidade certificados para fornecer orientação e avaliações para várias estruturas do setor. AWS Os profissionais do SAS criaram esse pacote de conformidade para permitir que o cliente se alinhe a um subconjunto da HIPAA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(A)	(A) Análise de risco (obrigatório). Realize uma avaliação precisa e completa dos possíveis riscos e vulnerabilidades à confidencialidade, integridade e disponibilidade de informações eletrônicas de saúde protegidas mantidas pela entidade abrangida.	annual-risk-assessment-performed (Verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implement e medidas de segurança suficient	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).		ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigató rio). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigató rio). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implement e medidas de segurança suficient es para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(1)(ii)(B)	(B) Gerenciamento de riscos (obrigatório). Implemente medidas de segurança suficientes para reduzir riscos e vulnerabilidades a um nível razoável e adequado para estar em conformidade com a Seção 164.306(a).	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônic as de saúde protegida s, conforme previsto no parágrafo (a) (4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônic as de saúde protegida s, conforme previsto no parágrafo (a) (4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônic as de saúde protegida s, conforme previsto no parágrafo (a) (4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônic as de saúde protegida s, conforme previsto no parágrafo (a) (4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(i)	Padrão (3)(i): segurança da força de trabalho. Implemente políticas e procedimentos para garantir que todos os membros da força de trabalho tenham acesso adequado às informações eletrônicas de saúde protegidas, conforme previsto no parágrafo (a)(4) desta seção, e para impedir que os membros da força de trabalho que não tenham acesso sob os termos do parágrafo (a)(4) desta seção obtenham acesso a informações de saúde eletrônicas protegidas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implement e procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçá vel). Implement e procedimentos para a autorizaç ão e/ou supervisã o dos membros da força de trabalho que trabalham com informações eletrônic as de saúde protegida s ou em locais onde elas possam ser acessadas.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implement e procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implement e procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(A)	(A) Autorização e/ou supervisão (endereçável). Implemente procedimentos para a autorização e/ou supervisão dos membros da força de trabalho que trabalham com informações eletrônicas de saúde protegidas ou em locais onde elas possam ser acessadas.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçá vel). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informaçõ es eletrônicas de saúde protegidas é adequado.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implemente procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implemente procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçá vel). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informaçõ es eletrônicas de saúde protegidas é adequado.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçá vel). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informaçõ es eletrônicas de saúde protegidas é adequado.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(B)	(B) Procedimento de liberação da força de trabalho (endereçável). Implement e procedimentos para determinar se o acesso de um membro da força de trabalho às informações eletrônicas de saúde protegidas é adequado.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(3)(ii)(C)	(C) Procedimentos de encerramento (endereçáveis). Implemente procedimentos para encerrar o acesso às informações eletrônicas de saúde protegidas quando o emprego de um membro da força de trabalho terminar ou conforme exigido pelas determinações feitas, conforme especificado no parágrafo (a)(3)(ii)(B) desta seção.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informações. Implemente políticas e procedimentos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informações eletrônicas de saúde protegidas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informações. Implemente políticas e procedimentos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informações eletrônicas de saúde protegidas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informaçõ es. Implemente políticas e procedime ntos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informaçõ es eletrônicas de saúde protegidas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informações. Implemente políticas e procedimentos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informações eletrônicas de saúde protegidas.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(i)	Padrão (4)(i): gerenciamento de acesso às informações. Implemente políticas e procedimentos que sejam consistentes com os requisitos aplicáveis da subparte E desta parte para autorizar o acesso às informações eletrônicas de saúde protegidas.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensação de assistência médica (obrigatório). Se uma câmara de compensação de assistência médica fizer parte de uma organização maior, a câmara de compensação deve implementar políticas e procedimentos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	ssm-document-not-p ublic	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	s3-bucket-acl-proh ibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriore s ao Identity and Access Managemen t (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(A)	(A) Isolamento das funções de câmara de compensaç ão de assistência médica (obrigató rio). Se uma câmara de compensaç ão de assistência médica fizer parte de uma organizaç ão maior, a câmara de compensação deve implementar políticas e procedime ntos que protejam suas informações eletrônicas de saúde protegidas do acesso não autorizado pela organização maior.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(B)	(B) Autorização de acesso (endereçável). Implemente políticas e procedimentos para conceder acesso às informações eletrônicas de saúde protegidas por meio do acesso a uma estação de trabalho, uma transação, um programa, um processo ou outro mecanismo.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorizaç ão de acesso da entidade, estabeleç am, documentem, revisem e modifique m o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(4)(ii)(C)	(C) Estabelecimento e modificação de acesso (endereçável). Implemente políticas e procedimentos que, com base nas políticas de autorização de acesso da entidade, estabeleçam, documentem, revisem e modifiquem o direito de acesso do usuário a uma estação de trabalho, uma transação, um programa ou um processo.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(A)	(A) Lembretes de segurança (endereçáveis). Atualizações periódicas de segurança.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(A)	(A) Lembretes de segurança (endereçáveis). Atualizações periódicas de segurança.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(A)	(A) Lembretes de segurança (endereçáveis). Atualizações periódicas de segurança.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(A)	(A) Lembretes de segurança (endereçáveis). Atualizações periódicas de segurança.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(B)	(B) Proteção contra software mal-intencionado (endereçável). Procedimentos para proteger, detectar e relatar software mal-intencionado.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(B)	(B) Proteção contra software mal-intencionado (endereçável). Procedimentos para proteger, detectar e relatar software mal-intencionado.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(B)	(B) Proteção contra software mal-intencionado (endereçável). Procedimentos para proteger, detectar e relatar software mal-intencionado.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(C)	(C) Monitoramento de login (endereçável). Procedimentos para monitorar tentativa s de login e relatar discrepâncias.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(C)	(C) Monitoramento de login (endereçável). Procedimentos para monitorar tentativa s de login e relatar discrepâncias.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(C)	(C) Monitoramento de login (endereçável). Procedimentos para monitorar tentativa s de login e relatar discrepâncias.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(5)(ii)(D)	(D) Gerenciamento de senhas (endereçá vel). Procedimentos para criar, alterar e proteger senhas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(6)(i)	Padrão (6)(i): procedimentos para incidentes de segurança. Implante políticas e procedimentos para lidar com incidentes de segurança.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(6)(ii)	(ii) Especificação de implementação: resposta e relatório (obrigatório). Identifiq ue e responda a incidentes de segurança suspeitos ou conhecidos; reduza, na medida do possível, os efeitos nocivos dos incidente s de segurança conhecidos pela entidade abrangida ; e documente os incidentes de segurança e seus resultados.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrências (por exemplo: incêndio, vandalismo, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônicas de saúde protegidas.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrências (por exemplo: incêndio, vandalismo, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônicas de saúde protegidas.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(i)	Padrão (7)(i): plano de contingência. Estabeleça (e implante, conforme necessário) políticas e procedimentos para responder a emergências ou outras ocorrênci as (por exemplo: incêndio, vandalism o, falha do sistema e desastres naturais) que danifiquem sistemas que contêm informações eletrônic as de saúde protegida s.	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(A)	(A) Plano de backup de dados (obrigatório). Estabeleça e implemente procedimentos para criar e manter cópias exatas recuperáveis de informações eletrônicas de saúde protegidas.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(B)	(B) Plano de recuperação de desastres (obrigatório). Estabeleça (e implante, conforme necessário) procedimentos para restaurar qualquer perda de dados.	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(7)(ii)(C)	(C) Plano de operação do modo de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para permitir a continuação de processos essenciais de negócios para proteger a segurança das informações eletrônicas de saúde protegidas enquanto a operação prossegue no modo de emergência.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(8)	Padrão (8): avaliação . Realize avaliaçõe s técnicas e não técnicas periodica mente, inicialme nte com base nos padrões implement ados sob esta regra e, posteriormente, em resposta às mudanças ambientai s ou operacionais que afetam a segurança das informações eletrônicas de saúde protegidas, que estabeleça até que ponto as políticas e procedimentos de segurança de uma entidade atendem aos requisitos desta subparte.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.308(a)(8)	Padrão (8): avaliação . Realize avaliações técnicas e não técnicas periodicamente, inicialmente com base nos padrões implementados sob esta regra e, posteriormente, em resposta às mudanças ambientais ou operacionais que afetam a segurança das informações eletrônicas de saúde protegidas, que estabeleça até que ponto as políticas e procedimentos de segurança de uma entidade atendem aos requisitos desta subparte.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-policy-no-stat ements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ec2-instance-no-pu blic-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informações eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especificado em 164.308(a)(4).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informações eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especificado em 164.308(a)(4).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informações eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especificado em 164.308(a)(4).	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	autoscaling-launch -config-public-ip- disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ecs-containers-rea donly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégi o mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em 164.308(a)(4).	s3-bucket-acl-proh ibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriore s ao Identity and Access Managemen t (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(1)	Padrão (a)(1): controle de acesso. Implemente políticas e procedimentos técnicos para sistemas eletrônicos de informações que mantenham informaçõ es eletrônicas de saúde protegidas para permitir o acesso somente às pessoas ou programas de software aos quais foram concedidos direitos de acesso, conforme especific ado em ¤ 164.308(a)(4).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(i)	(2) Especificações de implementação: (i) Identificação exclusiva do usuário (obrigatório). Atribua um nome e/ou número exclusivo s para identificar e rastrear a identidade do usuário.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
164.312(a)(2)(ii)	(ii) Procedimento de acesso de emergência (obrigatório). Estabeleça (e implemente, conforme necessário) procedimentos para obter as informações eletrônicas de saúde protegidas necessárias durante uma emergência.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônic as de saúde protegida s.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(a)(2)(iv)	(iv) Criptografia e decodificação (endereçável). Implemente um mecanismo para criptografar e descriptografar informações eletrônicas de saúde protegidas.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônic as de saúde protegida s.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônic as de saúde protegida s.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônic as de saúde protegida s.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônic as de saúde protegida s.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificações acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(b)	Padrão (b): controles de auditoria . Implemente mecanismos de hardware, software e/ou procedimentos que registrem e analisem a atividade em sistemas de informações que contenham ou usem informações eletrônicas de saúde protegidas.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
164.312(c)(1)	Padrão (c)(1): integridade. Implemente políticas e procedimentos para proteger as informações eletrônicas de saúde protegidas contra alterações ou destruição impróprias.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(1)	Padrão (c)(1): integridade. Implemente políticas e procedimentos para proteger as informaçõ es eletrônicas de saúde protegidas contra alterações ou destruição impróprias.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(1)	Padrão (c)(1): integridade. Implemente políticas e procedimentos para proteger as informaçõ es eletrônicas de saúde protegidas contra alterações ou destruição impróprias.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(1)	Padrão (c)(1): integridade. Implemente políticas e procedimentos para proteger as informaçõ es eletrônicas de saúde protegidas contra alterações ou destruição impróprias.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
164.312(c)(1)	Padrão (c)(1): integridade. Implemente políticas e procedimentos para proteger as informaçõ es eletrônicas de saúde protegidas contra alterações ou destruição impróprias.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(2)	(2) Especificação de implement ação: mecanismo de autenticação de informações eletrônicas de saúde protegidas (endereçá vel). Implemente mecanismos eletrônic os para confirmar que as informaçõ es eletrônicas de saúde protegidas não foram alteradas ou destruídas de forma não autorizada.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(2)	(2) Especificação de implement ação: mecanismo de autenticação de informações eletrônicas de saúde protegidas (endereçá vel). Implemente mecanismos eletrônic os para confirmar que as informaçõ es eletrônicas de saúde protegidas não foram alteradas ou destruídas de forma não autorizada.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
164.312(c)(2)	(2) Especificação de implement ação: mecanismo de autenticação de informações eletrônicas de saúde protegidas (endereçá vel). Implemente mecanismos eletrônic os para confirmar que as informaçõ es eletrônicas de saúde protegidas não foram alteradas ou destruídas de forma não autorizada.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(2)	(2) Especificação de implement ação: mecanismo de autenticação de informações eletrônicas de saúde protegidas (endereçá vel). Implemente mecanismos eletrônic os para confirmar que as informaçõ es eletrônicas de saúde protegidas não foram alteradas ou destruídas de forma não autorizada.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(c)(2)	(2) Especificação de implement ação: mecanismo de autenticação de informações eletrônicas de saúde protegidas (endereçá vel). Implemente mecanismos eletrônic os para confirmar que as informaçõ es eletrônicas de saúde protegidas não foram alteradas ou destruídas de forma não autorizada.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(d)	Padrão (d): autenticação de pessoa ou entidade. Implemente procedimentos para verificar se uma pessoa ou entidade que busca acesso a informações eletrônicas de saúde protegidas corresponde a que foi declarada.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(d)	Padrão (d): autenticação de pessoa ou entidade. Implemente procedimentos para verificar se uma pessoa ou entidade que busca acesso a informações eletrônicas de saúde protegidas corresponde a que foi declarada.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(d)	Padrão (d): autenticação de pessoa ou entidade. Implemente procedimentos para verificar se uma pessoa ou entidade que busca acesso a informações eletrônicas de saúde protegidas corresponde a que foi declarada.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(d)	Padrão (d): autenticação de pessoa ou entidade. Implemente procedimentos para verificar se uma pessoa ou entidade que busca acesso a informações eletrônicas de saúde protegidas corresponde a que foi declarada.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(d)	Padrão (d): autenticação de pessoa ou entidade. Implemente procedimentos para verificar se uma pessoa ou entidade que busca acesso a informações eletrônicas de saúde protegidas corresponde a que foi declarada.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônic as de saúde protegida s que estão sendo transmitidas por uma rede de comunicaç ões eletrônicas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônic as de saúde protegida s que estão sendo transmitidas por uma rede de comunicaç ões eletrônicas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônic as de saúde protegida s que estão sendo transmitidas por uma rede de comunicaç ões eletrônicas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônic as de saúde protegida s que estão sendo transmitidas por uma rede de comunicaç ões eletrônicas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(1)	Padrão (e)(1): segurança de transmissão. Implemente medidas técnicas de segurança para evitar o acesso não autorizado às informações eletrônicas de saúde protegidas que estão sendo transmitidas por uma rede de comunicações eletrônicas.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(i)	(i) Controles de integridade (endereçáveis). Implemente medidas de segurança para garantir que as informações eletrônicas de saúde protegidas que são transmitidas eletronicamente não sejam modificadas indevidamente sem serem detectadas até serem descartadas.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informaçõ es eletrônicas de saúde protegidas sempre que necessári o.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefinidas usadas para a negociação SSL quando é estabelecida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptores SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informaçõ es eletrônicas de saúde protegidas sempre que necessári o.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informaçõ es eletrônicas de saúde protegidas sempre que necessári o.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informaçõ es eletrônicas de saúde protegidas sempre que necessári o.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
164.312(e)(2)(ii)	(ii) Criptografia (endereçável). Implemente um mecanismo para criptografas informações eletrônicas de saúde protegidas sempre que necessário.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(1)	Padrão (b)(1): requisitos para planos de saúde coletivos . Exceto quando as únicas informações eletrônicas de saúde protegidas divulgadas a um patrocinador do plano são divulgada s de acordo com ¤ 164.504(f)(1)(ii) ou (iii), ou conforme autorizado em ¤ 164.508, um plano de saúde coletivo deve garantir que seus documentos estabeleçam que o patrocinador do plano proteja, de forma razoável e adequada, as informações eletrônicas de saúde protegidas criadas, recebidas, mantidas ou transmitidas para ou pelo patrocina dor do plano em seu nome.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	rds-snapshot-encrypted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo; (ii) garanta que a separação adequada exigida em ¤ 164.504(f)(2) (iii) seja apoiada por medidas de segurança razoáveis e apropriadas; (iii) garanta que qualquer	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	atendente, incluindo um subcontratado, a quem fornece essas informaçõ es concorda em implementar medidas de segurança razoáveis e apropriad as para proteger as informações; e (iv) relate ao plano de saúde do grupo qualquer incidente de segurança do qual tenha conhecimento.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implemente proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	ecs-containers-rea donly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégi o mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	s3-bucket-acl-proh ibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriore s ao Identity and Access Managemen t (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elb-predefined-sec urity-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configura ções de negociaçã o SSL predefini das usadas para a negociação SSL quando é estabelec ida uma conexão entre um cliente e seu balanceador de carga. As configura ções de negociaçã o SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmo s criptográficos de alta robustez. Essa regra exige que você defina uma política de segurança predefini da para os receptore s SSL. A política de

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	dynamodb-autoscali ng-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidad e de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidad e provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposiçõ es que exijam que o patrocinador do plano: (i) implement e proteções administr ativas, físicas e técnicas que protejam de forma razoável e adequada a confidenc ialidade, a integrida de e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	opensearch-node-to -node-encryption-c heck	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
164.314(b)(2)(i)	(2) Especificações de implementação (obrigatório). Os documentos do plano de saúde coletivo devem ser alterados para incorporar disposições que exijam que o patrocinador do plano: (i) implement e proteções administrativas, físicas e técnicas que protejam de forma razoável e adequada a confidencialidade, a integridade e a disponibilidade das informações eletrônicas de saúde protegidas que ele cria, recebe, mantém ou transmite em nome do plano de saúde coletivo;	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para segurança da HIPAA.

Práticas recomendadas operacionais para o IRS 1075

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos

usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o IRS 1075 e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do IRS 1075. Um controle do IRS 1075 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica dos pelo FIPS 140 e operar utilizand o os mais recentes módulos compatíve is com o FIPS 140. Esse requisito deve ser incluído no SLA.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dos pelo FIPS 140 e operar utilizando os mais recentes módulos compatíveis com o FIPS 140. Esse requisito deve ser incluído no SLA.		habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certificados pelo FIPS 140 e operar utilizando os mais recentes módulos compatíveis com o FIPS 140. Esse requisito deve ser incluído no SLA.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica dos pelo FIPS 140 e operar utilizand o os mais recentes módulos compatíve is com o FIPS 140. Esse requisito deve ser incluído no SLA.	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica dos pelo FIPS 140 e operar utilizand o os mais recentes módulos compatíve is com o FIPS 140. Esse requisito deve ser incluído no SLA.	opensearch-node-to -node-encryption-c heck	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica dos pelo FIPS 140 e operar utilizand o os mais recentes módulos compatíve is com o FIPS 140. Esse requisito deve ser incluído no SLA.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.3.1 Computação em nuvem d. Criptografia de dados em trânsito	O FTI deve ser criptografado em trânsito no ambiente de nuvem. Todos os mecanismos usados para criptografar o FTI devem ser certifica dos pelo FIPS 140 e operar utilizand o os mais recentes módulos compatíve is com o FIPS 140. Esse requisito deve ser incluído no SLA.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	dynamodb-table-enc rypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem e. Criptografia de dados em repouso	Criptografia de dados em repouso: o FTI deve ser criptografado enquanto estiver em repouso na nuvem usando o mecanismo de criptografia certificado pelo FIPS 140 mais recente. Esse requisito deve ser incluído no SLA.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem k. Autenticação multifator	As agências devem implementar autenticação multifatorial suficiente quando suas soluções em nuvem estiverem disponíveis na Internet (ou seja, quando houver acesso à solução em nuvem de fora da rede confiável da agência).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem k. Autenticação multifator	As agências devem implementar autenticação multifatorial suficiente quando suas soluções em nuvem estiverem disponíveis na Internet (ou seja, quando houver acesso à solução em nuvem de fora da rede confiável da agência).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem k. Autenticação multifator	As agências devem implementar autenticação multifatorial suficiente quando suas soluções em nuvem estiverem disponíveis na Internet (ou seja, quando houver acesso à solução em nuvem de fora da rede confiável da agência).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1 Computação em nuvem k. Autenticação multifator	As agências devem implementar autenticação multifatorial suficiente quando suas soluções em nuvem estiverem disponíveis na Internet (ou seja, quando houver acesso à solução em nuvem de fora da rede confiável da agência).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
3.3.1 Computação em nuvem i. Avaliação de risco:	A agência deve realizar uma avaliação anual dos controles de segurança e privacidade em vigor em todos os sistemas de informação utilizados para receber, processar, armazenar, acessar, proteger e/ou transmitir o FTI.	annual-risk-assessment-performed (verificação de processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	netfw-policy-rule-group-associated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.6 Limite e infraestrutura da rede	As agências devem implementar dispositivos de proteção de limites em toda a arquitetura do seu sistema, incluindo roteadores, firewalls, switches e sistemas de detecção de intrusão para proteger sistemas FTI e FTI.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (f)	Criar, ativar, modificar, desativar e remover contas de acordo com os pré-requisitos dos procedimentos de gerenciamento de contas da agência;	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (f)	Criar, ativar, modificar, desativar e remover contas de acordo com os pré-requisitos dos procedimentos de gerenciamento de contas da agência;	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
Gerenciamento de contas do AC-2 (f)	Criar, ativar, modificar, desativar e remover contas de acordo com os pré-requisitos dos procedimentos de gerenciamento de contas da agência;	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (f)	Criar, ativar, modificar , desativar e remover contas de acordo com os pré-requisitos dos procedimentos de gerenciamento de contas da agência;	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (f)	Criar, ativar, modificar, desativar e remover contas de acordo com os pré-requisitos dos procedimentos de gerenciamento de contas da agência;	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (g)	Monitorar o uso de contas	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	secretsmanager-secret-periodic-rotation	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação periódica ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido. O valor padrão é 90 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Gerenciamento de contas do AC-2 (j)	Revise as contas para se certificar de que há conformidade com os requisitos de gerenciamento de contas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
(CE-1) Gerenciamento automatizado de contas do sistema	Ofereça suporte ao gerenciamento de contas do sistema utilizando mecanismos automatizados.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
(CE-1) Gerenciamento automatizado de contas do sistema	Ofereça suporte ao gerenciamento de contas do sistema utilizando mecanismos automatizados.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
(CE-1) Gerenciamento automatizado de contas do sistema	Ofereça suporte ao gerenciamento de contas do sistema utilizando mecanismos automatizados.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
(CE-3): Desabilitar contas	Desabilite contas dentro de 120 dias quando elas: a. expirarem; b. não estiverem mais associadas a um usuário ou indivíduo; c. violarem a política organizacional; ou d. estiverem inativas por 120 dias para contas não privilegiadas e 60 dias para contas privilegiadas.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
(CE-12) Monitoramento de contas para uso atípico	Monitore contas do sistema para uso atípico definido pela agência; e relate o uso atípico de contas do sistema para funcionários ou funções definidas pela agência.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	iam-policy-no-stat ements-with-admin-access	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
Privilégio mínimo do AC-6	Empregue o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que sejam necessários para realizar as tarefas organizacionais atribuídas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17: Acesso remoto	Estabeleça e documente restrições de uso, requisitos de configuração/conexão e orientações de implementação para cada tipo de acesso remoto permitido; e autorize cada tipo de acesso remoto ao sistema antes de permitir tais conexões.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AT-1: Conscientização e treinamento	Forneça treinamento básico sobre segurança e privacidade aos usuários do sistema (incluindo gerentes, executivos seniores e prestadores de serviços)	security-awareness-program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
AU-2: Eventos de auditoria	Identifique os tipos de eventos que o sistema é capaz de registrar para oferecer suporte à função de auditoria	audit-log-policy-exists (verificação de processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-16: Registro em log de auditoria interorganizacional	Empregue métodos definidos pela agência para coordenar informações de auditoria definidas pela agência entre organizações externas quando as informações de auditoria forem transmitidas por meio dos limites organizac ionais.	audit-log-policy-e xists (verificação de processo)	Estabeleça e mantenha uma política de gerenciam ento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7: Monitoramento contínuo	Desenvolva uma estratégia de monitoramento contínuo em nível de sistema e implement e monitoramento contínuo de acordo com a estratégia de monitoramento contínuo em nível de organização: estabeleça métricas definidas pela agência a serem monitoradas; avaliações de controle contínuas de acordo com a estratégia de monitoramento contínuo; monitoram ento contínuo de métricas definidas pelo sistema e pela organização de acordo com a estratégia de monitoramento contínuo; correlaçã o e análise de informações geradas por avaliações e monitoramento de controle; ações de resposta para lidar	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	com os resultado s da análise da avaliação do controle e da informação de monitoramento; e relate anualmente o status de segurança e privacidade do sistema ao pessoal definido pela agência, no mínimo.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	aurora-resources-p rotected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	backup-plan-min-fr equency-and-min-re tention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyV alue parâmetros (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	backup-recovery-po int-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionD ays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documentação do sistema, incluindo documentação relacionada à segurança. b. Realize backups semanais das informações em nível de sistema contidas no sistema. c. Realize backups semanais da documentação do sistema, incluindo documentação relacionada à segurança e privacidade. d. Proteja a confidencialidade, integridade e disponibilidade das informações de backup.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	ec2-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	fsx-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documentação do sistema, incluindo documentação relacionada à segurança. b. Realize backups semanais das informações em nível de sistema contidas no sistema. c. Realize backups semanais da documentação do sistema, incluindo documentação relacionada à segurança e privacidade. d. Proteja a confidencialidade, integridade e disponibilidade das informações de backup.	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9: Backup do sistema	a. Realize backups semanais das informações em nível de usuário contidas na documenta ção do sistema, incluindo documenta ção relacionada à segurança. b. Realize backups semanais das informaçõ es em nível de sistema contidas no sistema. c. Realize backups semanais da documenta ção do sistema, incluindo documenta ção relacionada à segurança e privacidade. d. Proteja a confidenc ialidade, integrida de e disponibilidade das informações de backup.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2: Identificação e autenticação (usuários organizacionais) (CE-1) Autenticação multifator para contas privilegiadas	Implementar autenticação multifator para acesso a contas privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2: Identificação e autenticação (usuários organizacionais) (CE-1) Autenticação multifator para contas privilegiadas	Implementar autenticação multifator para acesso a contas privilegiadas	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2: Identificação e autenticação (usuários organizacionais) (CE-2) Autenticação multifator para contas não privilegiadas	Implementar autenticação multifator para acesso a contas não privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5: Gerenciamento do autenticador: (CE-1) Autenticação baseada em senha: para autenticação baseada em senha	Aplique as seguintes regras de composição e complexidade: 1. Imponha um tamanho mínimo de senha de quatorze (14) caracteres. 2. Imponha a complexidade mínima da senha para conter uma combinação de números, letras maiúsculas, letras minúsculas e caracteres especiais. 3. Imponha pelo menos uma (1) alteração de caractere quando novas senhas são selecionadas para uso. 4. Armazene e transmita somente senhas protegidas por criptografia. 5. Aplique restrições de vida útil à senha: i. Mínimo de um (1) dia e máximo de 90 dias. ii. As senhas das contas de serviço expirarão em 366 dias (inclusive).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PM-5: Inventário do sistema	Desenvolva e atualize continuamente um inventário de sistemas organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PM-5: Inventário do sistema	Desenvolva e atualize continuamente um inventário de sistemas organizacionais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PM-5: Inventário do sistema	Desenvolva e atualize continuamente um inventário de sistemas organizacionais.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PM-5: Inventário do sistema	Desenvolva e atualize continuamente um inventário de sistemas organizacionais.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-5: Monitoramento e verificação de vulnerabilidades	Monitore e verifique as vulnerabilidades no sistema e nas aplicações hospedadas a cada trinta (30) dias, antes de colocar um novo sistema de informações na rede da agência, para confirmar as ações de correção e quando novas vulnerabilidades que possam afetar o sistema forem identificadas e relatadas	vuln-scans-performed (verificação de processo)	Garanta que as verificações de vulnerabilidade sejam realizadas de acordo com seus requisitos de conformidade. A frequência da verificação, as ferramentas usadas e o uso dos resultados devem ser definidos pela sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10: Gerenciamento de configuração do desenvolvedor (e.)	Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10: Gerenciamento de configuração do desenvolvedor (e.)	Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10: Gerenciamento de configuração do desenvolvedor (e.)	Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-10: Gerenciamento de configuração do desenvolvedor (a) (c.)	Execute o gerenciamento de configuração durante o projeto, desenvolvimento, implementação e operação do sistema, componente ou serviço; implement e apenas alterações aprovadas pela organização no sistema, componente ou serviço;	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-4: Informações em recursos compartilhados do sistema	Evite transferências não autorizadas e não intencionais de informações por meio de recursos compartilhados do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessíveis ao público que estejam separados das redes organizacionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados de acordo com uma arquitetura de segurança organizacional.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessíveis ao público que estejam separados das redes organizacionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados de acordo com uma arquitetura de segurança organizacional.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessíveis ao público que estejam separados das redes organizacionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados de acordo com uma arquitetura de segurança organizacional.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessíveis ao público que estejam separados das redes organizacionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados de acordo com uma arquitetura de segurança organizacional.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	sagemaker-notebook -no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites	Monitore e controle as comunicações no limite externo do sistema e nos principais limites internos do sistema; implemente sub-redes para componentes do sistema acessívei s ao público que estejam separados das redes organizac ionais internas; e conecte-se a redes externas ou sistemas de informação somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os de acordo com uma arquitetura de segurança organizac ional.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limite (CE-9) Restrição do tráfego de comunicações de saída ameaçador	Detecte e negue o tráfego de comunicações de saída que representa uma ameaça aos sistemas externos; e audite a identidade de usuários internos associados a comunicações negadas.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limite (CE-9) Restrição do tráfego de comunicações de saída ameaçador	Detecte e negue o tráfego de comunicações de saída que representa uma ameaça aos sistemas externos; e audite a identidade de usuários internos associados a comunicações negadas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limite (CE-9) Restrição do tráfego de comunicações de saída ameaçador	Detecte e negue o tráfego de comunicações de saída que representa uma ameaça aos sistemas externos; e audite a identidade de usuários internos associados a comunicações negadas.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7: Proteção de limites (definida pelo IRS)	As agências devem implementar e gerenciar a proteção de limites (normalmente usando firewalls) nos limites de confiança. Cada limite de confiança deve ser monitorado e as comunicações por meio de cada limite devem ser controladas.	netfw-policy-rule-group-associated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.
SC-7: Proteção de limites (definida pelo IRS)	As agências devem implementar e gerenciar a proteção de limites (normalmente usando firewalls) nos limites de confiança. Cada limite de confiança deve ser monitorado e as comunicações por meio de cada limite devem ser controladas.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8: Proteção criptográfica de confidencialidade e integridade da transmissão (CE-1)	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de informações e detectar alterações nas informações durante a transmissão.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12: Gerenciamento e estabelecimento de chaves criptográficas	A agência deve estabelecer e gerenciar chaves criptográficas quando a criptografia é empregada no sistema de acordo com os seguintes requisitos de gerenciamento de chaves: NIST SP 800-57, recomendação para gerenciamento de chaves, para geração, distribuição, armazenamento, acesso e destruição de chaves.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12: Gerenciamento e estabelecimento de chaves criptográficas	A agência deve estabelecer e gerenciar chaves criptográficas quando a criptografia é empregada no sistema de acordo com os seguintes requisitos de gerenciamento de chaves: NIST SP 800-57, recomendação para gerenciamento de chaves, para geração, distribuição, armazenamento, acesso e destruição de chaves.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessários para cada uso criptográfico especificado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrizes para a seleção, configuração e uso de implementações de segurança da camada de transporte (TLS), criptografia em trânsito (criptografia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13: Proteção criptográfica	Implemente os tipos de criptografia a seguir, necessári os para cada uso criptográfico especific ado: mecanismo de criptografia validado pelo FIPS-140 mais recente, NIST 800-52, diretrize s para a seleção, configuração e uso de implementações de segurança da camada de transport e (TLS), criptografia em trânsito (criptogr afia de carga útil). O uso do SHA-1 para assinaturas digitais é proibido.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23: Autenticidade da sessão	Proteja a autenticidade das sessões de comunicação.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28: Proteção de informações em repouso (CE-1) Proteção criptográfica	Implemente mecanismos criptográficos para impedir a divulgação e modificação não autorizada do FTI em repouso nos sistemas de computação do usuário final (ou seja, computadores desktop, notebooks, dispositivos móveis, dispositivos de armazenamento portáteis e removíveis) em armazenamento não volátil.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessário ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessário ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessári o ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessári o ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrad o um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataform a. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataform a.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessário ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2: Correção de falhas (definida pelo IRS)	A agência deve garantir que, após a inicialização e conexão diárias à rede da agência, as estações de trabalho (conforme definido na política e incluindo conexões remotas usando estações de trabalho GFE) sejam verificadas para garantir que os patches mais recentes aprovados pela agência tenham sido aplicados e que quaisquer patches ausentes ou novos sejam aplicados conforme necessário ou verificados pelo menos a cada 24 horas (excluindo fins de semana, feriados, etc.)	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema	A organização: a. Monitora o sistema de informação para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; b. Identifica o uso não autorizado do sistema de informação por meio de [Atribuiç ão: técnicas e métodos definidos pela organização]; c. Implanta dispositivos de monitoramento: 1. Estrategicamente dentro do sistema de informação para coletar informações essenciais determina das pela organizaç ão; e 2. Em locais ad hoc dentro do sistema para rastrear tipos específic	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os de transaçõe s de interesse para a organizaç ão; d. Protege as informações obtidas de ferramentas de monitoramento de intrusões contra acesso, modificaç ão e exclusão não autorizados;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema	A organização: a. Monitora o sistema de informação para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; b. Identifica o uso não autorizado do sistema de informação por meio de [Atribuiç ão: técnicas e métodos definidos pela organização]; c. Implanta dispositivos de monitoramento: 1. Estrategicamente dentro do sistema de informação para coletar informações essenciais determina das pela organizaç ão; e 2. Em locais ad hoc dentro do sistema para rastrear tipos específic	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os de transaçõe s de interesse para a organizaç ão; d. Protege as informações obtidas de ferramentas de monitoramento de intrusões contra acesso, modificaç ão e exclusão não autorizados;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema	A organização: a. Monitora o sistema de informação para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; b. Identifica o uso não autorizado do sistema de informação por meio de [Atribuiç ão: técnicas e métodos definidos pela organização]; c. Implanta dispositivos de monitoramento: 1. Estrategicamente dentro do sistema de informação para coletar informações essenciais determina das pela organizaç ão; e 2. Em locais ad hoc dentro do sistema para rastrear tipos específic	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os de transaçõe s de interesse para a organizaç ão; d. Protege as informações obtidas de ferramentas de monitoramento de intrusões contra acesso, modificaç ão e exclusão não autorizados;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema	A organização: a. Monitora o sistema de informação para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; b. Identifica o uso não autorizado do sistema de informação por meio de [Atribuiç ão: técnicas e métodos definidos pela organização]; c. Implanta dispositivos de monitoramento: 1. Estrategicamente dentro do sistema de informação para coletar informações essenciais determina das pela organizaç ão; e 2. Em locais ad hoc dentro do sistema para rastrear tipos específic	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os de transaçõe s de interesse para a organizaç ão; d. Protege as informações obtidas de ferramentas de monitoramento de intrusões contra acesso, modificaç ão e exclusão não autorizados;		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema	A organização: a. Monitora o sistema de informação para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; b. Identifica o uso não autorizado do sistema de informação por meio de [Atribuiç ão: técnicas e métodos definidos pela organização]; c. Implanta dispositivos de monitoramento: 1. Estrategicamente dentro do sistema de informação para coletar informações essenciais determina das pela organizaç ão; e 2. Em locais ad hoc dentro do sistema para rastrear tipos específic	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os de transaçõe s de interesse para a organizaç ão; d. Protege as informações obtidas de ferramentas de monitoramento de intrusões contra acesso, modificaç ão e exclusão não autorizados;		
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/ portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4: Monitoramento do sistema (definido pelo IRS)	Todos os pontos/portais de acesso à internet devem capturar e reter, por pelo menos um ano, informações de cabeçalho de tráfego de entrada e saída, com exceção das conexões “anônimas” de internet autorizadas, conforme aprovado pelo CISO da agência.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7: Software, firmware e integridade da informação	Use ferramentas de verificação de integridade para detectar alterações não autorizadas nos seguintes softwares, firmware e informações: kernels do sistema, drivers, firmware (por exemplo, BIOS, UEFI), software (por exemplo, sistema operacional, aplicativos, middleware) e atributos de segurança.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7: Software, firmware e integridade da informação	Use ferramentas de verificação de integridade para detectar alterações não autorizadas nos seguintes softwares, firmware e informações: kernels do sistema, drivers, firmware (por exemplo, BIOS, UEFI), software (por exemplo, sistema operacional, aplicativos, middleware) e atributos de segurança.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7: Software, firmware e integridade da informação	Use ferramentas de verificação de integridade para detectar alteraçõe s não autorizad as nos seguintes softwares, firmware e informações: kernels do sistema, drivers, firmware (por exemplo, BIOS, UEFI), software (por exemplo, sistema operacional, aplicativ os, middlewar e) e atributos de segurança.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	dynamodb-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	ebs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	efs-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	rds-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12: Gerenciamento e retenção de informações	Gerencie e retenha as informações dentro e fora do sistema de acordo com as leis, ordens executivas, diretivas, regulamentos, políticas, padrões, diretrizes e requisitos operacionais aplicáveis.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o IRS 1075.

Práticas recomendadas operacionais para o K-ISMS

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre a Coreia — Sistema de Gerenciamento de Segurança da Informação (ISMS) e regras AWS gerenciadas do Config. Cada regra do Config se aplica a um recurso específico da AWS e está relacionada a um ou mais controles do Korea – ISMS. Um controle do Korea – ISMS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
1.2.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
1.2.1	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
2.1.3	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em

ID de controle	AWS Regra de configuração	Orientação
		uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciad as e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
2.1.3	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
2.3.3	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
2.3.3	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
2.5.1	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
2.5.1	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
2.5.1	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.5.1	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
2.5.1	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
2.5.1	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
2.5.3	iam-user-mfa-enabled	Ative essa regra para restringi r o acesso aos recursos na AWS nuvem. Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
2.5.3	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
2.5.3	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
2.5.4	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
2.5.5	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
2.5.5	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
2.5.5	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
2.6	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
2.6	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.
2.6	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
2.6	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
2.6	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
2.6	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
2.6	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
2.6	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
2.6	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
2.6	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
2.6	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
2.6	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
2.6	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
2.6	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
2.6	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
2.6	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
2.6	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
2.6	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
2.6	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
2.6	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
2.6.6	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
2.6.6	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
2.6.6	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
2.6.6	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
2.6.6	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
2.6.6	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.6.6	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
2.6.6	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
2.6.6	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
2.6.6	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
2.6.6	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
2.6.6	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
2.6.7	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
2.7	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
2.7	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.7	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.7	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
2.7	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
2.7	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
2.7	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
2.7	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
2.7	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
2.7	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
2.7	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.7	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
2.7	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.7	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
2.7	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.7	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
2.7	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.7	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.7	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
2.7	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.7	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
2.7	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
2.7	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
2.7	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
2.7	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.7.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
2.7.1	elb-predefined-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, os receptores SSL do Classic Elastic Load Balancing devem usar uma política de segurança predefinida. O Elastic Load Balancing oferece configurações de negociação SSL predefini das usadas para a negociaçã o SSL quando é estabelec ida uma conexão entre um cliente e seu balanceador de carga. As configurações de negociação SSL fornecem compatibilidade com uma ampla gama de clientes e usam algoritmos criptográ ficos de alta robustez. Essa regra exige que você defina uma política de segurança predefinida para os receptore s SSL. A política de segurança padrão é: ELB SecurityPolicy -TLS-1-2-2017-0. O valor real deve refletir as políticas da organização.
2.7.2	cmk-backing-key-rotation-en abled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográ fico.

ID de controle	AWS Regra de configuração	Orientação
2.7.2	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
2.8.5	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
2.8.5	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub
2.8.6	codebuild-project-envvar-aw scred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_ KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
2.8.6	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub
2.9.1	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.

ID de controle	AWS Regra de configuração	Orientação
2.9.1	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
2.9.1	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
2.9.1	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.9.2	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
2.9.2	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	AWS Regra de configuração	Orientação
2.9.2	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default: 80). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
2.9.2	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.
2.9.2	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determina do momento.

ID de controle	AWS Regra de configuração	Orientação
2.9.2	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.
2.9.3	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
2.9.3	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
2.9.3	elasticache-redis-cluster-automatic-backup-check	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.
2.9.3	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
2.9.3	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
2.9.3	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
2.9.3	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
2.9.3	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
2.9.4	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
2.9.4	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
2.9.4	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.
2.9.4	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
2.9.4	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
2.9.4	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
2.10.3	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
2.10.3	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
2.10.3	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.
2.10.3	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
2.10.3	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
2.10.5	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.10.5	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.10.5	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.10.5	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
2.10.5	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.10.5	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.10.5	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.10.5	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.10.8	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
2.10.8	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
2.11.2	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	AWS Regra de configuração	Orientação
2.11.3	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.
2.11.3	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	AWS Regra de configuração	Orientação
2.11.3	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
2.11.3	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelec idos. Isso pode ajudar a definir o número de solicitações que a função atende em determina do momento.

ID de controle	AWS Regra de configuração	Orientação
2.11.3	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	AWS Regra de configuração	Orientação
2.11.3	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
2,12	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
2,12	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
2,12	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2,12	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
2,12	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2,12	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
2,12	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
2,12	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balancead or de carga seja excluído de forma acidental ou mal-inten cionada, o que pode levar à perda de disponibilidade das aplicações.
2,12	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
2,12	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2,12	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
2,12	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
2,12	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2,12	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
2,12	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
2,12	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectivi dade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponi bilidade do gateway do cliente acarreta a perda de conectivi dade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.
2,12	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2,12	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir os requisitos da organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para K-ISMS.

Práticas recomendadas operacionais para o balanceamento de carga

Esse pacote de conformidade contém AWS Config regras baseadas no balanceamento de carga interno. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para balanceamento de carga.

Práticas recomendadas operacionais para o Registro

Esse pacote de conformidade contém AWS Config regras com base no login. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para registro em log.

Práticas recomendadas operacionais para serviços de gerenciamento e governança

Esse pacote de conformidade contém AWS Config regras baseadas nos Serviços de Gerenciamento e Governança. Para obter mais informações, consulte Gestão e Governança em AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de gerenciamento e governança.

Práticas recomendadas operacionais para o Aviso 655 do MAS

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre o Aviso 655 da Autoridade Monetária de Cingapura (MAS) — Cyber Hygiene e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do MAS Notice 655 — Cyber Hygiene. Um controle de Aviso 655 do MAS, Cyber Hygiene pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
4.1	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra

ID de controle	AWS Regra de configuração	Orientação
		requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
4.1	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
4.1	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
4.1	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
4.1	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
4.1	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
4.1	iam-user-mfa-enabled	Ative essa regra para restringi r o acesso aos recursos na AWS nuvem. Essa regra garante que a autentica ção multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidente s de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
4.1	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
4.1	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
4.1	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
4.1	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
4.1	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
4.1	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
4.2	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
4.2	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
4.2	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
4.2	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.2	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
4.2	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
4.2	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.
4.2	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificaç ão de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	AWS Regra de configuração	Orientação
4.3	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
4.3	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
4.3	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
4.3	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	AWS Regra de configuração	Orientação
4.4	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
4.4	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
4.4	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
4.4	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
4.4	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
4.4	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
4.4	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
4.4	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
4.4	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
4.4	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
4.4	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
4.4	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
4.4	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
4.4	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
4.4	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
4.4	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.

ID de controle	AWS Regra de configuração	Orientação
4.4	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.
4.4	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
4.4	netfw-policy-default-action-fragment-packets	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras sem estado e stateful para filtrar pacotes e fluxos de tráfego. Usar como padrão uma ação Transmitir pode permitir tráfego não intencional.

ID de controle	AWS Regra de configuração	Orientação
4.4	netfw-policy-default-action-full-packets	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras sem estado e stateful para filtrar pacotes e fluxos de tráfego. Usar como padrão uma ação Transmitir pode permitir tráfego não intencion al.
4.4	netfw-policy-rule-group-ass ociated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.
4.4	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	AWS Regra de configuração	Orientação
4.4	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
4.4	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.4	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
4.4	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
4.4	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
4.4	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
4.4	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
4.4	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
4.4	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
4.4	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
4.4	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
4.4	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
4.4	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
4.4	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	AWS Regra de configuração	Orientação
4.4	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
4.4	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
4.5	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
4.5	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
4.5	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
4.5	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
4.6	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
4.6	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
4.6	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
4.6	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
4.6	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
4.6	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o Aviso 655 do MAS.

Práticas recomendadas operacionais para as TRMG da MAS

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre as Diretrizes de Gerenciamento de Risco Tecnológico (TRMG) da Autoridade Monetária de Cingapura (MAS) de janeiro de 2021 e as regras gerenciadas AWS do Config. Cada regra de AWS Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles MAS TRMG. Um controle das TRMG da MAS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
3.3.1	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.
5.4.3	codebuild-project-envvar-aw scred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_ KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.
5.4.3	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild. AWS Use OAuth em vez de tokens de acesso

ID de controle	AWS Regra de configuração	Orientação
		pessoal ou credenciais de login para conceder autorizaç ão para acessar nossos repositórios do Bitbucket. GitHub
6.1.1	codebuild-project-envvar-aw scred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_ KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.
6.1.2	codebuild-project-envvar-aw scred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_ KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	AWS Regra de configuração	Orientação
6.1.4	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
6.1.4	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
6.1.4	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
6.2.1	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
6.3.1	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.
6.4.5	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
6.4.5	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
6.4.5	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
6.4.5	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográ fico.

ID de controle	AWS Regra de configuração	Orientação
6.4.5	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
6.4.5	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
6.4.5	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
6.4.5	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
6.4.5	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
6.4.5	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
6.4.5	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
6.4.5	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
6.4.6	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
6.4.6	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
6.4.6	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.
6.4.6	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
6.4.6	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
6.4.7	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
6.4.7	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
6.4.7	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
6.4.7	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
6.4.7	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
6.4.7	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
6.4.7	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
6.4.7	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
6.4.7	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
6.4.8	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.
6.4.8	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
6.4.8	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
7.2.1	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
7.2.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
7.4.1	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
7.4.1	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
7.4.1	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
7.4.1	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
7.4.1	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.

ID de controle	AWS Regra de configuração	Orientação
7.4.1	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
7.5.5	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
7.5.5	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
7.5.5	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
7.5.5	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
7.5.5	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
7.5.5	elasticache-redis-cluster-automatic-backup-check	Quando os backups automátic os estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamen te. O backup pode ser retido por vários dias, conforme especificado pela organizaç ão. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
7.5.5	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
7.5.5	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatiz ados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
7.5.5	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
7.5.5	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
7.5.7	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
7.5.7	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
7.5.7	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
7.5.7	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
7.5.7	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
7.5.7	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
7.5.7	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
8.1.1	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
8.1.1	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
8.1.1	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
8.1.1	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
8.1.1	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
8.1.1	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
8.1.1	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
8.1.1	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	AWS Regra de configuração	Orientação
8.1.2	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
8.1.2	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
8.1.2	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
8.1.2	opensearch-data-node-fault-tolerance	O Amazon OpenSearch Service (OpenSearch Service) exige pelo menos três nós de dados para alta disponibi lidade e tolerância a falhas. A implantação de um domínio OpenSearch de serviço com pelo menos três nós de dados garante as operações do cluster se um nó falhar.

ID de controle	AWS Regra de configuração	Orientação
8.1.2	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
8.1.3	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	AWS Regra de configuração	Orientação
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integridade aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.
8.1.3	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
8.1.3	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
8.4.1	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
8.4.1	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
8.4.1	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
8.4.1	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
8.4.1	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizan do a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	AWS Regra de configuração	Orientação
8.4.1	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
8.4.1	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
8.4.1	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
8.4.1	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	AWS Regra de configuração	Orientação
8.4.1	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
8.4.1	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
8.4.2	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
8.4.2	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizan do a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
8.4.2	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
8.4.2	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
8.4.2	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
8.4.2	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.
8.4.4	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
8.5.4	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
8.5.4	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.
9.1.1	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
9.1.1	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperad o de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégi os elevados.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
9.1.1	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
9.1.1	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
9.1.1	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
9.1.1	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
9.1.1	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
9.1.1	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
9.1.1	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programaç ão regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
9.1.1	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
9.1.1	secretsmanager-secret-periodic-rotation	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação periódica ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido. O valor padrão é 90 dias.
9.1.1	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credencias, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.2	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.2	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
9.1.2	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.2	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
9.1.2	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
9.1.2	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
9.1.3	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
9.1.3	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
9.1.3	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
9.1.3	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
9.1.3	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
9.1.3	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
9.1.3	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
9.1.3	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
9.1.3	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
9.1.3	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
9.1.4	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
9.1.5	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
9.1.5	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
9.1.5	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
9.1.5	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
9.1.6	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.7	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
9.1.7	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.7	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
9.1.7	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.1.7	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
9.1.7	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
9.2.1	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
9.2.1	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
9.2.1	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
9.2.1	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.2.1	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
9.2.2	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
9.2.2	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
9.2.2	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
9.2.2	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
9.2.2	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.2.2	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
9.3.1	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
9.3.1	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
9.3.1	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
9.3.1	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
9.3.1	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
9.3.1	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
9.3.1	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
9.3.1	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
9.3.1	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
9.3.1	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.1.1	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.1.1	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
10.1.1	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
10.1.1	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
10.1.1	dynamodb-table-encrypted-km s	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
10.1.1	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
10.1.1	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
10.1.1	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.1.1	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
10.1.1	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.1.1	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
10.1.1	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
10.1.1	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
10.1.1	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
10.1.1	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
10.1.1	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
10.1.1	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
10.1.1	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
10.1.1	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
10.2.1	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
10.2.1	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
10.2.1	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	AWS Regra de configuração	Orientação
10.2.2	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	AWS Regra de configuração	Orientação
10.2.3	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.
10.2.3	cmk-backing-key-rotation-en abled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográ fico.

ID de controle	AWS Regra de configuração	Orientação
10.2.3	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programad as para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessári a, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
11.1.1 (a)	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (a)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.1 (a)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
11.1.1 (a)	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (a)	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
11.1.1 (a)	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
11.1.1 (a)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (a)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
11.1.1 (b)	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
11.1.1 (b)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
11.1.1 (b)	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.1.1 (b)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.1.1 (b)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
11.1.1 (b)	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
11.1.1 (b)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
11.1.1 (b)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
11.1.1 (b)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.
11.1.1 (b)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.
11.1.1 (b)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
11.1.1 (b)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
11.1.1 (b)	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.1 (b)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
11.1.1 (b)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
11.1.1 (b)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
11.1.1 (b)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
11.1.1 (b)	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.1 (b)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.1 (b)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.
11.1.1 (b)	vpc-sg-open-only-to-authori zed-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.3	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
11.1.3	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
11.1.3	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.1.3	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
11.1.3	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
11.1.3	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
11.1.3	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
11.1.3	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
11.1.3	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
11.1.3	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
11.1.3	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
11.1.3	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
11.1.3	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.3	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptogra fia em repouso para ajudar a protegê-los.
11.1.3	root-account-hardware-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
11.1.3	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
11.1.3	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
11.1.3	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
11.1.3	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
11.1.3	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
11.1.3	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
11.2.1	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
11.2.2	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
11.2.2	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.2.2	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
11.2.2	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
11.2.2	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
11.2.2	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.
11.2.2	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
11.2.2	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
11.2.2	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
11.2.2	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
11.2.2	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
11.2.2	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
11.2.2	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
11.2.2	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
11.2.4	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.2.4	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11.2.4	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
11.2.4	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
11.2.4	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
11.2.4	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
11.2.4	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
11.2.4	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
11.2.4	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
11.2.4	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
11.2.4	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
11.2.4	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.
11.3.1	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	AWS Regra de configuração	Orientação
11.3.5	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
11.3.5	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
11.3.5	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
11.4.2	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
11.4.2	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.
11.4.2	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
11.4.2	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
11.5.2	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
12.1.1	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
12.1.1	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
12.1.1	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
12.2.2	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
12.2.2	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
12.2.2	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
12.2.2	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
12.2.2	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
12.2.2	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
12.2.2	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
12.2.2	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	AWS Regra de configuração	Orientação
12.2.2	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
12.2.4	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
12.2.4	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
12.2.5	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
12.2.5	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
12.2.5	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
12.3.2	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
12.3.2	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
14.1.2	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
14.1.2	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
14.1.2	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
14.1.2	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
14.1.2	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
14.1.2	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
14.1.2	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	AWS Regra de configuração	Orientação
14.1.2	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
14.1.2	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
14.1.3	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
14.1.3	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
14.1.3	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
14.1.3	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS
14.2.2	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
14.2.2	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
14.2.2	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
14.2.2	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
14.2.2	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
14.2.2	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
14.2.2	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
14.2.2	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
14.2.2	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
14.2.2	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
14.2.2	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
14.2.2	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
14.2.6	dynamodb-table-encrypted-km s	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
14.2.6	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
14.2.6	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
14.2.6	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
14.2.6	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
14.2.6	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
14.2.6	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
14.2.6	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o MAS TRMG.

Práticas recomendadas operacionais para o monitoramento

Este pacote de conformidade contém AWS Config regras baseadas no monitoramento interno. AWS Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para monitoramento.

Práticas recomendadas de operação para as TRMG do NBC

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre a estrutura das Diretrizes de Gerenciamento de Risco Tecnológico (TRM) do Banco Nacional do Camboja (NBC) e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a uma ou mais Diretrizes do NBC TRM. Uma Diretriz de TRM do NBC pode estar relacionada a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do framework das Diretrizes de Gerenciamento de Risco Tecnológico (TRM) do Banco Nacional do Camboja (NBC), que pode ser acessado aqui: National Bank of Cambodia: Technology Risk Mangement Guidelines.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorizaç ão da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs		Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorizaç ão da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentaç ão efetiva de deveres - Alteração dos nomes de usuário e/ ou senhas padrão dos sistemas e proibição do compartil hamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorizaç ão da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentaç ão efetiva de deveres - Alteração dos nomes de usuário e/ ou senhas padrão dos sistemas e proibição do compartil hamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorizaç ão da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentaç ão efetiva de deveres - Alteração dos nomes de usuário e/ ou senhas padrão dos sistemas e proibição do compartil hamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorizaç ão da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentaç ão efetiva de deveres - Alteração dos nomes de usuário e/ ou senhas padrão dos sistemas e proibição do compartil hamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(d)	d) Entre os controles importantes que precisam ser considerados estão: - Um processo sistemático de aplicação e autorização da criação de IDs de usuário e da matriz de controle de acesso - A realização de uma avaliação de risco e a concessão de direitos de acesso com base na mesma. - Implementação de controle de acesso baseado em perfis projetado para garantir a segmentação efetiva de deveres - Alteração dos nomes de usuário e/ou senhas padrão dos sistemas e proibição do compartilhamento de IDs de usuário e senhas de contas genéricas - Modificação dos direitos de acesso sempre que houver uma mudança no	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	perfil ou na responsabilidade e remoção dos direitos de acesso na cessação do emprego/contrato - Processos para notificar em tempo hábil a função de segurança da informação sobre adições, exclusões e mudanças de perfil do usuário - Reconciliação periódica de IDs de usuários em um sistema e usuários reais que precisam ter acesso e exclusão de IDs desnecessários, se houver - Auditoria, registro em log e monitoramento do acesso aos ativos de TI por todos os usuários e - Consideração da desativação de IDs de usuários de aplicações essenciais que estejam em licença prolongada		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditávei s.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(f)	f) Para fins de responsabilidade, certifique-se de que os usuários e ativos de TI sejam identificados de forma exclusiva e que suas ações sejam auditáveis.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		as senhas e outras informações administr ativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		o), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeir o), MinimumPa sswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	wafv2-logging-enab led	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariave lmente possuem a capacidade de infligir danos graves aos sistemas financeir os que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisi onados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1(h)	h) Administradores de sistemas, agentes de segurança, programadores e funcionários que realizam operações essenciais invariavelmente possuem a capacidade de infligir danos graves aos sistemas financeiros que mantêm ou operam em virtude de suas funções de trabalho e acesso privilegiado. Os funcionários com direitos elevados de acesso ao sistema devem ser supervisionados atentamente e devem ter todas as suas atividades nos sistemas registradas em log, pois possuem conhecimento interno e os recursos para contornar os controles e procedimentos de segurança dos sistemas. Algumas das práticas de controle e segurança	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	enumeradas abaixo precisam ser consideradas: - Implementar a autenticação de dois fatores para usuários privilegiados - Instituir controles robustos sobre o acesso remoto de usuários privilegiados - Restringir o número de usuários privilegi ados - Conceder acesso privilegi ado com base na “necessidade de ter” ou na “necessid ade de fazer” - Manter o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados - Garantir que usuários privilegiados não tenham acesso aos registros em log de sistemas nos quais suas atividades estão sendo capturadas - Conduzir auditoria s regulares ou revisões gerenciai		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s dos registros em log - Proibir o compartilhamento de IDs privilegiados e os códigos de acesso - Impedir que fornecedores e prestadores de serviço obtenham acesso privilegi ado aos sistemas sem supervisão e monitoramento rigorosos - Proteger os dados de backup contra acesso não autorizado		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(a)	a) O BFI deve instalar dispositivos de segurança de rede, como firewalls , software antivírus /antimalware, bem como sistemas de detecção e prevenção de intrusões, em pontos críticos de sua infraestrutura de TI, para proteger os perímetros da rede.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(a)	a) O BFI deve instalar dispositivos de segurança de rede, como firewalls , software antivírus /antimalware, bem como sistemas de detecção e prevenção de intrusões, em pontos críticos de sua infraestrutura de TI, para proteger os perímetros da rede.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(a)	a) O BFI deve instalar dispositivos de segurança de rede, como firewalls , software antivírus /antimalware, bem como sistemas de detecção e prevenção de intrusões, em pontos críticos de sua infraestrutura de TI, para proteger os perímetros da rede.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	acm-certificate-ex piration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	wafv2-logging-enab led	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	ec2-instance-no-pu blic-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		ser atribuídas a uma VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-bucket-public-w rite-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	autoscaling-launch -config-public-ip- disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectados (incluindo protocolos de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestrutura de processamento de informações - Os sistemas na rede devem ser autenticados e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(c)	c) Devem ser implementados controles para garantir a segurança das informaçõ es nas redes e a proteção dos serviços conectados contra o acesso não autorizad o. Em particular, os seguintes itens devem ser considerados: - Responsabilidades e procedimentos para o gerenciamento de equipamentos de rede devem ser estabelec idos - A responsab ilidade operacion al pelas redes deve ser separada das operações de computador, quando apropriado - Controles especiais devem ser estabelecidos para proteger a confidencialidade e integridade dos dados que passam por redes públicas ou redes sem fio e para proteger	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os sistemas e as aplicações conectado s (incluindo protocolo s de criptografia de rede ao se conectar a sistemas/redes não confiáveis). - O registro em log e o monitoramento apropriados devem ser aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevante s para a segurança da informação - As atividades de gerenciamento devem ser coordenadas de perto para otimizar o serviço para a organização e garantir que os controles sejam aplicados de forma consistente em toda a infraestr utura de processam ento de informações - Os sistemas na rede devem ser autentica dos e - As conexões não confiáveis do		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	sistema com a rede devem ser restritas		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2(e)	e) Os serviços de rede podem variar de simples largura de banda não gerenciada a serviços sofisticados, como VPN, voz sobre IP, VSAT, etc. Os recursos de segurança dos serviços de rede devem ser: - Tecnologia aplicada à segurança dos serviços de rede, como autenticação, criptografia e controles de conexão de rede - Parâmetros técnicos necessários para uma conexão segura com os serviços de rede de acordo com as regras de segurança e conexão de rede e - Procedimentos para o uso do serviço de rede para restringir o acesso aos serviços ou aplicações de rede, quando necessário	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
3.1.3(e)	e) Use criptografia para proteger os canais de comunicação entre o dispositivo de acesso remoto e a instituição para restringir os riscos relacionados à falsificação de rede.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizada s por meio do acesso remoto	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(g)	g) Mantenha registros em log para comunicações de acesso remoto. Os registros em logs devem incluir a data, a hora, o usuário, a localização do usuário, a duração e a finalidade de todo o acesso remoto, incluindo todas as atividades realizadas por meio do acesso remoto	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(i)	i) Aplique o processo de autenticação de dois fatores para acesso remoto (por exemplo, cartão de token baseado em PIN com um gerador de senha aleatório único ou PKI baseada em token)	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(i)	i) Aplique o processo de autenticação de dois fatores para acesso remoto (por exemplo, cartão de token baseado em PIN com um gerador de senha aleatório único ou PKI baseada em token)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(i)	i) Aplique o processo de autenticação de dois fatores para acesso remoto (por exemplo, cartão de token baseado em PIN com um gerador de senha aleatório único ou PKI baseada em token)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3(i)	i) Aplique o processo de autenticação de dois fatores para acesso remoto (por exemplo, cartão de token baseado em PIN com um gerador de senha aleatório único ou PKI baseada em token)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabilidades aplicáveis aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantação de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabilidades aplicáveis aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantação de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabi lidades aplicávei s aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantaç ão de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabilidades aplicáveis aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantação de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabilidades aplicáveis aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantação de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4(c)(e)	c) O processo de gerenciamento de patches deve incluir aspectos como: - Determinar métodos de obtenção e validação de patches para garantir que o patch seja de uma fonte autorizada - Identificar vulnerabilidades aplicáveis aos aplicativos e sistemas usados pela organização - Avaliar o impacto comercial da implementação de patches (ou não implementar um patch específico) - Garantir que os patches sejam testados - Descrever métodos para implantar patches, por exemplo, automaticamente - Relatórios sobre o status da implantação de patches em toda a organização e - Incluindo métodos para lidar com a falha na implantaç	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ão de um patch (por exemplo, reimplant ação do patch). e) Os BFIs devem implantar ferrament as automatizadas de gerenciamento de patches e ferrament as de atualização de software para todos os sistemas para os quais essas ferrament as estejam disponíve is e sejam seguras		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(d)(e)	d) O gerenciamento adequado de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribui r, retirar e destruir chaves criptográ ficas e) Todas as chaves criptográficas devem ser protegida s contra modificações e perdas. Além disso, as chaves secretas e privadas precisam de proteção contra uso não autorizad o e divulgação. O equipamento usado para gerar, armazenar e arquivar chaves deve ser fisicamente protegido.	kms-cmk-not-schedu led-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programad as para exclusão, caso alguma delas sido programada de maneira não intencion al.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(d)(e)	d) O gerenciamento adequado de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribui r, retirar e destruir chaves criptográ ficas e) Todas as chaves criptográficas devem ser protegida s contra modificações e perdas. Além disso, as chaves secretas e privadas precisam de proteção contra uso não autorizad o e divulgação. O equipamento usado para gerar, armazenar e arquivar chaves deve ser fisicamente protegido.	cmk-backing-key-ro tation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(d)(e)	d) O gerenciamento adequado de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribui r, retirar e destruir chaves criptográ ficas e) Todas as chaves criptográficas devem ser protegida s contra modificações e perdas. Além disso, as chaves secretas e privadas precisam de proteção contra uso não autorizad o e divulgação. O equipamento usado para gerar, armazenar e arquivar chaves deve ser fisicamente protegido.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(d)(e)	d) O gerenciamento adequado de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribui r, retirar e destruir chaves criptográ ficas e) Todas as chaves criptográficas devem ser protegida s contra modificações e perdas. Além disso, as chaves secretas e privadas precisam de proteção contra uso não autorizad o e divulgação. O equipamento usado para gerar, armazenar e arquivar chaves deve ser fisicamente protegido.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de comando devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de comando devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de comando devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de comando devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedime ntos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativ os - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizad os obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de compra devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de compra devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5(f)	f) Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para: - gerar chaves para diferentes sistemas criptográficos e diferentes aplicativos - emitir e obter certificados de chave pública - distribuir chaves às entidades pretendidas, incluindo como as chaves devem ser ativadas quando recebidas - armazenar chaves, incluindo como os usuários autorizados obtêm acesso às chaves - alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser alteradas e como isso será feito - lidar com chaves comprometidas - revogação de chaves,	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	incluindo chaves de compra devem ser retiradas ou desativadas, por exemplo, quando as chaves foram comprometidas ou quando um usuário deixa uma organização (nesse caso, as chaves também devem ser arquivadas) - recuperando chaves perdidas ou corrompidas - fazendo backup ou arquivando chaves - destruindo chaves e - registrando e auditando atividades relacionadas ao gerenciamento de chaves.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6(a)	a) O BFI deve implantar uma combinação de ferramentas automatizadas e técnicas manuais para realizar um VA abrangente periodicamente. Em sistemas externos baseados na web, o escopo do VA deve incluir vulnerabilidades comuns da web, como injeção de SQL e script entre sites da web.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6(a)	a) O BFI deve implantar uma combinação de ferramentas automatizadas e técnicas manuais para realizar um VA abrangente periodicamente. Em sistemas externos baseados na web, o escopo do VA deve incluir vulnerabilidades comuns da web, como injeção de SQL e script entre sites da web.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6(a)	a) O BFI deve implantar uma combinação de ferramentas automatizadas e técnicas manuais para realizar um VA abrangente periodicamente. Em sistemas externos baseados na web, o escopo do VA deve incluir vulnerabilidades comuns da web, como injeção de SQL e script entre sites da web.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6(c)	c) O BFI deve estabelecer um processo para remediar os problemas identificados em VA e PT e realizar a revalidação subsequente da remediação para validar se as lacunas foram totalmente solucionadas.	vuln-mitigated-accepted (verificação de processo)	Garanta que as vulnerabilidades recém-identificadas sejam corrigidas ou documentadas como riscos aceitos. As vulnerabilidades devem ser corrigidas ou aceitas como riscos de acordo com os requisitos de conformidade da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6(f)	f) A função de segurança deve fornecer atualizações de status em relação ao número de vulnerabilidades críticas e não mitigadas, para cada departamento/divisão, e planejar a mitigação para a gerência sênior periodicamente.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.8	Treinamento e conscientização de usuários.	security-awareness-program-exists (verificação de processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fo nte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificad ores de integrida de, hashes criptográ ficos). Além disso, as políticas devem minimizar a distribui ção de informaçõ es confidenciais, incluindo impressõe s que contenham as informações.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.10(b)	b) Informações confidenciais, como documentação do sistema, código-fonte do aplicativo e dados de transações de produção, devem ter controles mais amplos para evitar alterações (por exemplo, verificadores de integridade, hashes criptográficos). Além disso, as políticas devem minimizar a distribuição de informações confidenciais, incluindo impressões que contenham as informações.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associado s às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantaç ão.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(h)	h) Para minimizar os riscos associados às mudanças, os BFIs devem realizar backups dos sistemas ou aplicações afetados antes da mudança. Os BFIs devem estabelecer um plano de reversão para reverter para uma versão anterior do sistema ou aplicação se um problema for encontrado durante ou após a implantação.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investiga ções e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividade s que são realizadas durante o processo de migração.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investiga ções e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividade s que são realizadas durante o processo de migração.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investiga ções e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividade s que são realizadas durante o processo de migração.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investiga ções e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividade s que são realizadas durante o processo de migração.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investiga ções e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividade s que são realizadas durante o processo de migração.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1(k)	k) Os registros em log de auditoria e segurança são informações úteis que facilitam as investigações e a solução de problemas. O BFI deve garantir que a instalação de registro em log esteja habilitada para registrar as atividades que são realizadas durante o processo de migração.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.3(a)	a) Desenvolva e implemente processos para prevenir, detectar, analisar e responder a incidentes de segurança da informação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.3(a)	a) Desenvolva e implemente processos para prevenir, detectar, analisar e responder a incidentes de segurança da informação.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	dynamodb-autoscali ng-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidad e de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidad e provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores importantes associados à manutenção da alta disponibilidade do sistema, capacidade adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
3.3.1(a)	a) Considere fatores importantes associados à manutenção da alta disponibilidade do sistema, capacidade adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	dynamodb-throughpu t-limit-check	Habilite essa regra para garantir que a capacidade de throughput provision ada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidad e de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalm ente os parâmetro s AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentag e (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
3.3.1(a)	a) Considere fatores important es associados à manutenção da alta disponibilidade do sistema, capacidad e adequada, desempenho confiável, tempo de resposta rápido e escalabilidade como parte do projeto do sistema.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	wafv2-logging-enab led	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identificados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsabilidade e a identificação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegiados. f) Garanta que o registro em log e o monitoramento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(a)(b)(c)(f)(j)	a) Garanta que os registros de acesso do usuário sejam identific ados e registrados em log de forma exclusiva para fins de auditoria e revisão. b) Tenha a responsab ilidade e a identific ação do acesso não autorizado. c) Permita o registro em log de auditoria das atividades do sistema realizadas por usuários privilegi ados. f) Garanta que o registro em log e o monitoram ento adequados sejam aplicados para permitir o registro em log e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação. j) Garanta que o registro em log de eventos estabeleça a base para a automação	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	de sistemas de monitoramento capazes de gerar relatórios e alertas consolidados sobre segurança do sistema.		
3.4(f)	f) Garanta que o registro em log e o monitoramento apropriados sejam aplicados para permitir o registro e a detecção de ações que possam afetar ou sejam relevantes para a segurança da informação.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante: - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identificador do sistema - Registros de tentativas de acesso ao sistema bem-sucedidas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alterações na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante: - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identificador do sistema - Registros de tentativas de acesso ao sistema bem-sucedidas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alterações na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identificador do sistema - Registros de tentativas de acesso ao sistema bem-sucedidas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alterações na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executadas por usuários em aplicativos e transações on-line com clientes		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4(g)	g) Certifique-se de que os registros de eventos incluam, quando relevante : - IDs de usuário - Atividades do sistema - Datas, hora e detalhes dos principais eventos, por exemplo, login e desconexão - Identidade ou localização do dispositivo, se possível, e identific ador do sistema - Registros de tentativa s de acesso ao sistema bem-suced idas e rejeitadas - Registros de dados bem-sucedidos e rejeitados e outras tentativas de acesso a recursos - Alteraçõe s na configuração do sistema - Uso de privilégios - Uso de utilitários e aplicativos do sistema - Arquivos acessados e tipo de acesso - Endereços de rede e protocolo	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s - Alarmes gerados pelo sistema de controle de acesso e - Registros de transações executada s por usuários em aplicativos e transações on-line com clientes		
3.6.1(a)(h)	a) Os BFIs precisam garantir medidas de segurança adequadas para suas aplicaçõe s web e tomar medidas de mitigação razoáveis contra vários riscos de segurança da web. h) Os BFIs precisam garantir medidas de segurança adequadas para suas aplicaçõe s web e tomar medidas de mitigação razoáveis contra vários riscos de segurança da web.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(a)(h)	a) Os BFIs precisam garantir medidas de segurança adequadas para suas aplicaçõe s web e tomar medidas de mitigação razoáveis contra vários riscos de segurança da web. h) Os BFIs precisam garantir medidas de segurança adequadas para suas aplicaçõe s web e tomar medidas de mitigação razoáveis contra vários riscos de segurança da web.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisito s de segurança associados a seus sistemas de internet banking e outros sistemas relevante s e adotar uma solução de criptogra fia considerando o grau de confidenc ialidade e integridade exigido.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.6.1(b)	b) Os BFIs precisam avaliar os requisito s de segurança associados a seus sistemas de internet banking e outros sistemas relevante s e adotar uma solução de criptogra fia considerando o grau de confidenc ialidade e integridade exigido.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisito s de segurança associados a seus sistemas de internet banking e outros sistemas relevante s e adotar uma solução de criptogra fia considerando o grau de confidenc ialidade e integridade exigido.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
3.6.1(b)	b) Os BFIs precisam avaliar os requisito s de segurança associados a seus sistemas de internet banking e outros sistemas relevante s e adotar uma solução de criptogra fia considerando o grau de confidenc ialidade e integridade exigido.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
3.6.1(b)	b) Os BFIs precisam avaliar os requisitos de segurança associados a seus sistemas de internet banking e outros sistemas relevantes e adotar uma solução de criptografia considerando o grau de confidencialidade e integridade exigido.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(d)	d) Os BFIs que fornecem serviços de internet banking devem responder a condições incomuns de tráfego de rede/desempenho do sistema e a um aumento repentino na utilização de recursos do sistema, o que pode ser uma indicação de um ataque de DDoS. Consequentemente, o sucesso de qualquer ação preventiva e reativa depende da implantação de ferramentas apropriadas para detectar, monitorar e analisar anomalias em redes e sistemas com eficácia.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(d)	d) Os BFIs que fornecem serviços de internet banking devem responder a condições incomuns de tráfego de rede/desempenho do sistema e a um aumento repentino na utilização de recursos do sistema, o que pode ser uma indicação de um ataque de DDoS. Consequentemente, o sucesso de qualquer ação preventiva e reativa depende da implantação de ferramentas apropriadas para detectar, monitorar e analisar anomalias em redes e sistemas com eficácia.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(d)	d) Os BFIs que fornecem serviços de internet banking devem responder a condições incomuns de tráfego de rede/ desempenho do sistema e a um aumento repentino na utilização de recursos do sistema, o que pode ser uma indicação de um ataque de DDoS. Consequentemente, o sucesso de qualquer ação preventiva e reativa depende da implantação de ferramentas apropriadas para detectar, monitorar e analisar anomalias em redes e sistemas com eficácia.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(d)	d) Os BFIs que fornecem serviços de internet banking devem responder a condições incomuns de tráfego de rede/ desempenho do sistema e a um aumento repentino na utilização de recursos do sistema, o que pode ser uma indicação de um ataque de DDoS. Consequentemente, o sucesso de qualquer ação preventiva e reativa depende da implantação de ferramentas apropriadas para detectar, monitorar e analisar anomalias em redes e sistemas com eficácia.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(d)	d) Os BFIs que fornecem serviços de internet banking devem responder a condições incomuns de tráfego de rede/ desempenho do sistema e a um aumento repentino na utilização de recursos do sistema, o que pode ser uma indicação de um ataque de DDoS. Consequentemente, o sucesso de qualquer ação preventiva e reativa depende da implantação de ferramentas apropriadas para detectar, monitorar e analisar anomalias em redes e sistemas com eficácia.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1(e)	e) Os BFIs precisam avaliar regularmente as vulnerabilidades de segurança da informação e avaliar a eficácia do framework existente de gerenciamento de riscos de segurança de TI, fazendo os ajustes necessários para garantir que as vulnerabilidades emergentes sejam tratadas em tempo hábil. Essa avaliação também deve ser conduzida como parte de qualquer alteração material.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.4(a)(b)	a) Restrinja o acesso à internet e segmente os sistemas críticos do ambiente geral de TI. b) Reduza a superfície de ataque e as vulnerabilidades.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para NBC TRMG.

Práticas recomendadas operacionais para o NERC CIP BCSI

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os Padrões de Proteção de Infraestrutura Crítica da North American Electric Reliability Corporation (NERC CIP) para BES Cyber System Information (BCSI), CIP-004-7 e CIP-011-3 e regras gerenciadas. AWS Config Cada regra AWS do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles NERC CIP aplicáveis ao BCSI. Um controle do NERC CIP pode estar relacionado a várias regras do

Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar , verificar e revogar o acesso provision ado ao BCSI referente aos “Sistemas aplicáveis” identific ados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivam ente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios da Amazon. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de OpenSearch painéis e autenticação básica HTTP para Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	acesso provisionado deve ser considerado o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associados, chaves de criptografia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizado de acordo com a Parte 4.1.) com base na necessidade, conforme determinado pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provisionado ao BCSI eletrônico		informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar , verificar e revogar o acesso provision ado ao BCSI referente aos “Sistemas aplicáveis” identific ados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivam ente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-004-7-R6-Parte 6.1	Cada entidade responsável deve implementar um ou mais programas documentados de gerenciamento de acesso para autorizar, verificar e revogar o acesso provisionado ao BCSI referente aos “Sistemas aplicáveis” identificados na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information, que incluem coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R6 do CIP-004-7 — Gerenciamento de acesso ao BES Cyber System Information. Para ser considerado acesso ao BCSI no contexto desse requisito, um indivíduo deve ter a capacidade de obter e usar o BCSI. O acesso provisionado deve ser considerado	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	o resultado de ações específicas tomadas para fornecer a um indivíduo os meios de acessar o BCSI (por exemplo, pode incluir chaves físicas ou cartões de acesso, usuários e direitos e privilégios associado s, chaves de criptogra fia). Parte 6.1: antes do provisionamento, autorize (a menos que já esteja autorizad o de acordo com a Parte 4.1.) com base na necessidade, conforme determina do pela entidade responsável, exceto nas Circunstâncias Excepcionais do CIP: 6.1.1. Acesso eletrônico provision ado ao BCSI eletrônic o		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner . Habilitar a verificaç ão de imagens em repositórios do ECR adiciona uma camada de verificaç ão da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	ecr-private-tag-immutability-enabled	Habilite a imutabilidade de tags do Elastic Container Repository (ECR) para evitar que as tags de imagem em suas imagens do ECR sejam sobrescritas. Anteriormente, as tags podiam ser substituídas, exigindo metodologias manuais para identificar uma imagem de forma exclusiva.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service em uma Amazon VPC permite a comunicaç ão segura entre a Amazon OpenSearc h e outros serviços dentro da Amazon VPC sem a necessida de de um gateway de internet, dispositi vo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificaç ões acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	sagemaker-endpoint -configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-cluster-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informaçõ es documenta das que incluam coletivamente cada uma das partes dos requisitos aplicávei s na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	rds-instance-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de sua(s) instância(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	redshift-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) do Amazon Redshift.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CIP-011-3-R1-Parte 1.2	Cada entidade responsável deve implementar um ou mais programas de proteção de informações documentadas que incluam coletivamente cada uma das partes dos requisitos aplicáveis na Tabela R1 da CIP-011-3 – Proteção de informações. Parte 1.2: método(s) para proteger e lidar com segurança com o BCSI para mitigar os riscos de comprometer a confidencialidade.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para NERC CIP BCSI.

Práticas recomendadas operacionais para o NCSC Cloud Security Principles

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os Princípios de Segurança em Nuvem do Centro Nacional de Segurança Cibernética (NCSC) do Reino Unido e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do NCSC Cloud Security Principles do Reino Unido. Um controle do NCSC Cloud Security Principles do Reino Unido pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do NCSC Cloud Security Principles do Reino Unido (Centro Nacional de Segurança Cibernética | Diretriz de segurança na nuvem), com essas informações licenciadas do setor público sob a Open Government License v3.0. A Open Government Licence está disponível aqui: Open Government Licence for public sector information.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadamente protegidas contra adulteração e espionagem.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
1. Proteção de dados em trânsito	As redes de trânsito de dados do usuário devem ser adequadam ente protegidas contra adulteração e espionagem.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliênc ia de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
2. Proteção e resiliênc ia de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2. Proteção e resiliência de ativos	Seus dados (e os ativos que os armazenam ou processam) devem ser protegidos adequadamente.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
5. Segurança operacional	Os serviços devem ser operados e gerenciados de forma a impedir, detectar ou prevenir ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7. Desenvolvimento seguro	Os serviços em nuvem devem ser projetados, desenvolvidos e implantados de forma a minimizar e mitigar as ameaças à sua segurança.	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do privilégio mínimo, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegiado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7. Desenvolvimento seguro	Os serviços em nuvem devem ser projetados, desenvolvidos e implantados de forma a minimizar e mitigar as ameaças à sua segurança.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7. Desenvolvimento seguro	Os serviços em nuvem devem ser projetados, desenvolvidos e implantados de forma a minimizar e mitigar as ameaças à sua segurança.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibi lizar ferramentas para gerenciar com segurança o uso do serviço.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibi lizar ferramentas para gerenciar com segurança o uso do serviço.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibi lizar ferramentas para gerenciar com segurança o uso do serviço.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibi lizar ferramentas para gerenciar com segurança o uso do serviço.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
9. Gerenciar usuário com segurança	Os provedores devem disponibilizar ferramentas para gerenciar com segurança o uso do serviço.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	rds-instance-iam-authentication-enabled	Garanta que uma autenticação do AWS Identity and Access Management (IAM) esteja habilitada nas instâncias do Amazon Relational Database Service (Amazon RDS) para controlar o acesso a sistemas e ativos. Isso força o tráfego de rede de e para o banco de dados a ser criptografado usando o Secure Sockets Layer (SSL). Você não precisa armazenar as credenciais de usuário no banco de dados, porque a autenticação é gerenciada externamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10. Identidade e autenticação	O acesso às interfaces de serviço deve ser restrito a indivíduos autenticados e autorizados.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ecs-container-insi ghts-enabled	O monitoramento é uma parte important e da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Elastic Container Service (ECS) e de suas AWS soluções. O Container Insights também fornece informações de diagnóstico, como falhas de reinicial ização de contêiner , para ajudar a isolar problemas e resolvê-l os rapidamente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ecs-containers-non privileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ecs-containers-rea donly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégi o mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identificadas e defendidas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11. Proteção de interface externa	Todas as interfaces externas ou menos confiáveis do serviço devem ser identific adas e defendidas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
12. Administração segura de serviços	Os provedores de nuvem devem reconhecer o alto valor dos sistemas de administração.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13. Informações de auditoria para os usuários	Os provedores devem fornecer os logs necessários para monitorar o acesso ao seu serviço e os dados contidos nele.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
13. Informações de auditoria para os usuários	Os provedores devem fornecer os logs necessários para monitorar o acesso ao seu serviço e os dados contidos nele.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13. Informações de auditoria para os usuários	Os provedores devem fornecer os logs necessários para monitorar o acesso ao seu serviço e os dados contidos nele.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
13. Informações de auditoria para os usuários	Os provedores devem fornecer os logs necessários para monitorar o acesso ao seu serviço e os dados contidos nele.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para os princípios de segurança em nuvem do NCSC.

Práticas recomendadas operacionais para a Estrutura de Avaliação Cibernética do NCSC

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os controles da Estrutura de Avaliação Cibernética (CAF) do Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) e as regras

gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles CAF do NCSC do Reino Unido. Um controle da CAF do NCSC do Reino Unido relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro do NCSC da CAF do Reino Unido (diretriz do Centro Nacional de Segurança Cibernética | NCSC CAF), com essas informações licenciadas do setor público sob a Open Government License v3.0. A Open Government Licence está disponível aqui: Open Government Licence for public sector information.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
A3.a Gestão de ativos	Tudo o que é necessário para fornecer, manter ou apoiar redes e sistemas de informação necessários para a operação de funções essenciais é determinado e compreendido. Isso inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte (como energia ou resfriamento).	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
A3.a Gestão de ativos	Tudo o que é necessário para fornecer, manter ou apoiar redes e sistemas de informação necessári	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	os para a operação de funções essenciais é determinado e compreendido. Isso inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte (como energia ou resfriamento).		instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
A3.a Gestão de ativos	Tudo o que é necessário para fornecer, manter ou apoiar redes e sistemas de informação necessários para a operação de funções essenciais é determinado e compreendido. Isso inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte (como energia ou resfriamento).	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
A3.a Gestão de ativos	Tudo o que é necessário para fornecer, manter ou apoiar redes e sistemas de informação necessários para a operação de funções essenciais é determinado e compreendido. Isso inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte (como energia ou resfriamento).	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
A3.a Gestão de ativos	Tudo o que é necessário para fornecer, manter ou apoiar redes e sistemas de informação necessários para a operação de funções essenciais é determinado e compreendido. Isso inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de suporte (como energia ou resfriamento).	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.a Autenticação, autorização e verificação de identidade	Os processos de verificação, autenticação e autorização são realizados de forma robusta o acesso às redes e sistemas de informação que suportam sua função essencial.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
B2.b Gerenciamento de dispositivos	Você conhece e confia totalmente nos dispositivos usados para acessar suas redes, sistemas de informação e dados que suportam sua função essencial.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.b Gerenciamento de dispositivos	Você conhece e confia totalmente nos dispositivos usados para acessar suas redes, sistemas de informação e dados que suportam sua função essencial.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	codebuild-project-environment-privileged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegi ado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	ecs-containers-non privileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	secretsmanager-sec ret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credenciais, pois isso pode violar o princípio do menor privilégio. Essa regra permite que você defina um valor para unusedFor Days (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegiados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.c Gerenciamento de usuários privilegi ados	É possível gerenciar de perto o acesso privilegiado de usuários a redes e sistemas de informação que oferecem suporte à função.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B2.d Identity and Access Management (IAM)	É possível garantir um bom gerenciamento e manutenção do controle de identidade e acesso das suas redes e sistemas de informação com a função essencial.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.a Detalhamento dos dados	Você tem uma boa compreensão dos dados importantes para a operação da função essencial , onde eles são armazenados, para onde viajam e como a indisponibilidade ou o acesso, modificação ou exclusão não autorizados prejudicariam a função essencial . Isso também se aplica a terceiros que armazenam ou acessam dados importantes para a operação de funções essenciais.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada . Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.b Dados em trânsito	Você protegeu o trânsito de dados importantes para a operação da função essencial. Isso inclui a transferência de dados para terceiros.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	sagemaker-endpoint -configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	cmk-backing-key-ro tation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B3.c Dados armazenados	Você protegeu os dados armazenados importantes para a operação da função essencial.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciai s. A superfície de ataque é minimizad a e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciai s. A superfície de ataque é minimizad a e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.a Proteja usando o Design	Você projeta a segurança na rede e nos sistemas de informação que oferecem suporte à operação de funções essenciais. A superfície de ataque é minimizada e a operação da função essencial não é afetada pela exploração de uma única vulnerabilidade.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.b Proteja a configuração	Você configura com segurança a rede e os sistemas de informação que oferecem suporte à operação de funções essenciais.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.b Proteja a configuração	Você configura com segurança a rede e os sistemas de informação que oferecem suporte à operação de funções essenciais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.b Proteja a configuração	Você configura com segurança a rede e os sistemas de informação que oferecem suporte à operação de funções essenciais.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.b Proteja a configuração	Você configura com segurança a rede e os sistemas de informação que oferecem suporte à operação de funções essenciais.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.c Proteja o gerenciamento	Você gerencia a rede e os sistemas de informação da sua organização que oferecem suporte à operação de funções essenciais para habilitar e manter a segurança.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.c Proteja o gerenciamento	Você gerencia a rede e os sistemas de informação da sua organização que oferecem suporte à operação de funções essenciais para habilitar e manter a segurança.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.c Proteja o gerenciamento	Você gerencia a rede e os sistemas de informação da sua organização que oferecem suporte à operação de funções essenciais para habilitar e manter a segurança.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B4.d. Vulnerability Management	Você gerencia vulnerabilidades conhecidas em sua rede e sistemas de informação para evitar impactos adversos na função essencial.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.b Criado para resiliência	Você projeta a rede e os sistemas de informação que oferecem suporte à sua função essencial para ser resilient e a incidentes de segurança cibernéti ca. Os sistemas são adequadamente segregados, e as limitações de recursos são mitigadas.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.b Criado para resiliência	Você projeta a rede e os sistemas de informação que oferecem suporte à sua função essencial para ser resilient e a incidentes de segurança cibernéti ca. Os sistemas são adequadamente segregados, e as limitações de recursos são mitigadas.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
B5.b Criado para resiliência	Você projeta a rede e os sistemas de informação que oferecem suporte à sua função essencial para ser resilient e a incidentes de segurança cibernéti ca. Os sistemas são adequadamente segregados, e as limitações de recursos são mitigadas.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
B5.c Backups	Você mantém os backups atuais acessíveis e seguros dos dados e informações necessários para recuperar a operação de sua função essencial.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	dynamodb-throughpu t-limit-check	Habilite essa regra para garantir que a capacidade de throughput provision ada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidad e de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalm ente os parâmetro s AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentag e (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identificar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identificar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.a Cobertura de monitoramento	As fontes de dados que você inclui em seu monitoramento permitem identific ar em tempo hábil eventos de segurança que podem afetar a operação de sua função essencial.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.b Proteção dos logs	Você mantém os dados de registro em log com segurança e concede acesso de leitura somente às contas com necessidades comerciais. Nenhum funcionário poderá modificar ou excluir dados de registro em log no período de retenção acordado e, depois desse tempo, eles devem ser excluídos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	guardduty-non-arch ived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classific ando as descobert as por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégi as e prioridades de correção. Essa regra permite que você defina opcionalm ente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificaç ões acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	wafv2-logging-enab led	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.c Geração de alertas	As evidências de possíveis incidente s de segurança presentes em seus dados de monitoram ento são identificadas de forma confiável e acionam alertas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.d Identificação de incidentes de segurança	Você contextualiza os alertas conhecendo a ameaça e seus sistemas para identificar os incidentes de segurança que exigem alguma forma de resposta.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.d Identificação de incidentes de segurança	Você contextualiza os alertas conhecendo a ameaça e seus sistemas para identificar os incidentes de segurança que exigem alguma forma de resposta.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.e Ferramentas e habilidades de monitoramento	As habilidades, ferramentas e funções da equipe de monitoramento, incluindo aquelas terceirizadas, devem refletir os requisitos de governança e relatórios, as ameaças esperadas e as complexidades dos dados da rede ou do sistema que eles precisam usar. A equipe de monitoramento tem conhecimento das funções essenciais que precisam ser protegidas.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.e Ferramentas e habilidades de monitoramento	As habilidades, ferramentas e funções da equipe de monitoramento, incluindo aquelas terceirizadas, devem refletir os requisito s de governanç a e relatórios, as ameaças esperadas e as complexid ades dos dados da rede ou do sistema que eles precisam usar. A equipe de monitoramento tem conhecimento das funções essenciai s que precisam ser protegidas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C1.e Ferramentas e habilidades de monitoramento	As habilidades, ferramentas e funções da equipe de monitoramento, incluindo aquelas terceirizadas, devem refletir os requisito s de governanç a e relatórios, as ameaças esperadas e as complexid ades dos dados da rede ou do sistema que eles precisam usar. A equipe de monitoramento tem conhecimento das funções essenciai s que precisam ser protegidas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C2.a Anormalidades do sistema para detecção de ataques	Você define exemplos de anormalidades no comportamento do sistema que fornecem formas práticas de detectar atividades maliciosas que, de outra forma, seriam difíceis de identificar.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
C2.a Anormalidades do sistema para detecção de ataques	Você define exemplos de anormalidades no comportamento do sistema que fornecem formas práticas de detectar atividades maliciosas que, de outra forma, seriam difíceis de identificar.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
D1.c Testes e exercícios	Sua organização realiza exercícios para testar planos de resposta, usando incidentes anteriores que afetaram sua (e outras) organização e cenários que se baseiam na inteligência contra ameaças e na sua avaliação de riscos.	response-plan-exists-maintained (Verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.
D1.c Testes e exercícios	Sua organização realiza exercícios para testar planos de resposta, usando incidentes anteriores que afetaram sua (e outras) organização e cenários que se baseiam na inteligência contra ameaças e na sua avaliação de riscos.	response-plan-tested (Verificação do processo)	Teste os planos de recuperação e resposta a incidentes. Isso pode ajudar a saber se o plano será eficaz durante um incidente e se alguma lacuna ou atualização precisa ser resolvida.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para a estrutura de avaliação cibernética do NCSC.

Práticas recomendadas operacionais para serviços de rede e entrega de conteúdo

Esse pacote de conformidade contém AWS Config regras baseadas em serviços de rede e entrega de conteúdo. Para obter mais informações, consulte Rede e entrega de conteúdo em AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de rede e entrega de conteúdo.

Práticas recomendadas operacionais para o NIST 800-53 rev 4

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 800-53 e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles NIST 800-53. Um controle do NIST 800-53 pode estar relacionado a várias regras de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Esse pacote de conformidade foi validado pela AWS Security Assurance Services LLC (AWS SAS), que é uma equipe de avaliadores de segurança qualificados do setor de cartões de pagamento (QSAs), profissionais certificados pela HITRUST Common Security Framework (CCSFPs) e profissionais de conformidade certificados para fornecer orientação e avaliações para várias

estruturas do setor. AWS Os profissionais do SAS criaram esse pacote de conformidade para permitir que um cliente se alinhe a um subconjunto do NIST 800-53.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	secretsmanager-scheduled-rotation-success-verificar	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-group-membership-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(1)	A organização aplica mecanismos automatizados para oferecer suporte ao gerenciamento de contas do sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(3)	O sistema de informações desativa automaticamente as contas inativas após [Atribuição: período definido pela organização].	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todos Regiões da AWS para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(4)	O sistema de informações audita automaticamente as ações de criação, modificação, habilitação, desabilitação e remoção da conta, além de criar uma notificação [Atribuição: perfis ou pessoas definidas pela organização].	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(12)(a)	A organização: a. Monitora as contas do sistema de informaçõ es em busca de [Atribuição: uso atípico definido pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(12)(a)	A organização: a. Monitora as contas do sistema de informaçõ es em busca de [Atribuição: uso atípico definido pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(f)	A organização: f. Cria, habilita, modifica, desabilita e remove contas do sistema de informações de acordo com [Atribuição: procedimentos ou condições definidos pela organização].	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	s3- bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da Conta da AWS que acessou um bucket, endereço IP e horário do evento do Amazon S3.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(g)	A organização: g. Monitora o uso de contas do sistema de informações.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	secretsmanager-scheduled-rotation-success-verificar	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-group-membership-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			informações administrativas sobre cada entidade principal.
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-group-has-users-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformidade com os requisitos de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-2(j)	A organização: j. Analisa as contas quanto à conformid ade com os requisito s de gerenciamento de contas [Atribuição: frequência definida pela organização].	iam-user-no-policies-verificar	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3- bucket-public-writ e-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-no-policies-verificar	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3- bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-user-group-membership-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			informações administrativas sobre cada entidade principal.
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-group-has-users-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-3	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e aos recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ec2- instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas intercone ctados com base em [Atribuição: políticas de controle dos fluxos de informaçã o definidas pela organização].	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4	O sistema de informações impõe autorizações aprovadas para o controle do fluxo de informações dentro do sistema e entre sistemas interconectados com base em [Atribuição: políticas de controle dos fluxos de informação definidas pela organização].	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			informações administrativas sobre cada entidade principal.
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-group-has-users-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-5c	A organização: c. Define as autorizações de acesso ao sistema de informações para oferecer suporte à separação de deveres.	iam-user-no-policies-verificar	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizad os para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3- bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	codebuild-project-envvar-awscred-verificar	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-unused-credentials-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm, as senhas e outras

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			informações administrativas sobre cada entidade principal.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-group-has-users-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-group-membership-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-user-no-policies-verificar	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6	A organização emprega o princípio de privilégio mínimo, permitindo apenas acessos autorizados para usuários (ou processos que atuem em nome dos usuários) que são necessários para realizar as tarefas atribuídas de acordo com missões da organização e funções comerciais.	iam-no-inline-policy-verificar	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-6(10)	O sistema de informações impede que usuários não privilegiados executem funções privilegiadas, incluindo desabilitar, contornar ou alterar as proteções ou contramedidas de segurança implement adas.	iam-root-access-key-verificar	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(1)	O sistema de informações monitora e controla os métodos de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidenc ialidade e a integrida de das sessões de acesso remoto.	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	alb-http-drop-invalid-habilitado para cabeçalho	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-17(2)	O sistema de informações implementa mecanismos de criptografia para proteger a confidencialidade e a integridade das sessões de acesso remoto.	elb-tls-https-listeners-somente	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-17(3)	O sistema de informações roteia todos os acessos remotos por meio de pontos de controle de acesso à rede gerenciados por [Atribuição: número definido pela organização].	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AC-21(b)	A organização: b. Emprega [Atribuição: mecanismos automatizados ou processos manuais definidos pela organização] para ajudar os usuários a tomar decisões de compartilhamento ou colaboração de informações.	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	api-gw-execution-logging-habilitado	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da Conta da AWS que acessou um bucket, endereço IP e horário do evento do Amazon S3.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informaçõ es é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organizaç ão]; d. Determina que os seguintes eventos devem ser auditados no sistema de informaçã o: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequênci a da auditoria (ou situação que exige) para cada evento identificado].	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todos Regiões da AWS para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	s3- bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-2(a)(d)	A organização: a. Determina se o sistema de informações é capaz de auditar os seguintes eventos: [Atribuição: eventos auditáveis definidos pela organização]; d. Determina que os seguintes eventos devem ser auditados no sistema de informação: [Atribuição: eventos auditados definidos pela organização (o subconjunto dos eventos auditáveis definidos na AU-2 a.) junto com a frequência da auditoria (ou situação que exige) para cada evento identificado].	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	api-gw-execution-logging-habilitado	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da Conta da AWS que acessou um bucket, endereço IP e horário do evento do Amazon S3.
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Manag ement Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todos Regiões da AWS para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	s3- bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informações que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associados ao evento.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-3	O sistema de informações gera registros de auditoria que contêm informaçõ es que estabelecem que tipo de evento ocorreu, quando o evento ocorreu, onde o evento ocorreu, a origem do evento, o resultado do evento e a identidade de quaisquer indivíduos ou sujeitos associado s ao evento.	wafv2-logging-enab led	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-6(1)(3)	(1) A organização emprega mecanismos automatizados para integrar processos de revisão, análise e geração de relatórios de auditoria para apoiar os processos organizacionais de investigação e resposta a atividades suspeitas. (3) A organização analisa e correlaciona registros de auditoria em diferentes repositórios para obter consciência situacional em toda a organização.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-7(1)	O sistema de informações fornece recursos para processar registros de auditoria para eventos de interesse com base em [Atribuição: campos de auditoria definidos pela organização nos registros de auditoria].	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-7(1)	O sistema de informações fornece recursos para processar registros de auditoria para eventos de interesse com base em [Atribuição: campos de auditoria definidos pela organização nos registros de auditoria].	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU-9	O sistema de informações protege as informações e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
AU-9	O sistema de informações protege as informações e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-9(2)	O sistema de informação faz backup dos registros de auditoria [Atribuição: frequência definida pela organização] em um sistema ou componente do sistema fisicamente diferente do sistema ou componente que está sendo auditado.	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-11	A organização retém registros de auditoria para [Atribuição: período definido pela organização consistente com a política de retenção de registros] para fornecer suporte para after-the-fact investigações de incidentes de segurança e atender aos requisitos regulatórios e organizacionais de retenção de informações.	cw-loggroup-retention-period-verificar	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	api-gw-execution-logging-habilitado	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da Conta da AWS que acessou um bucket, endereço IP e horário do evento do Amazon S3.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidad e de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informaçõ es definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidad e de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informaçõ es definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Manag ement Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Management Console e chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todos Regiões da AWS para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	s3- bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
AU-12(a)(c)	O sistema de informações: (a) Fornece capacidade de geração de registros de auditoria para os eventos auditáveis definidos na AU-2 a. em [Atribuição: componentes do sistema de informações definido pela organização]; c. Gera registros de auditoria para os eventos definidos em AU-2 (d) com o conteúdo definido em AU-3.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	ec2- instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CA-7(a)(b)	A organização desenvolve uma estratégia de monitoramento contínuo e implement a um programa de monitoramento contínuo que inclui: a. O estabelec imento de [Atribuiç ão: métricas definidas pela organização] a serem monitorad as; b. O estabelec imento de [Atribuição: frequências definidas pela organização] para monitoram ento e [Atribuição: frequências definidas pela organização] para avaliações que oferecem suporte a esse monitoramento.	rds-enhanced-monit oring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibi lidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2- -check managedinstance-as sociation-compliance-status	Use o AWS Systems Manager Associati ons para ajudar no inventário de plataformas e aplicativ os de software em uma organizaç ão. AWS Systems Manager atribui um estado de configura ção às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacion al, instalações de software, configura ções de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	ec2- volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada . Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-2	A organizaç ão desenvolve, documenta e mantém, sob controle de configuração, uma configuração básica atual do sistema de informações.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-7(a)	A organização: a. Configura o sistema de informações para fornecer somente os recursos essenciais.	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-7(a)	A organização: a. Configura o sistema de informações para fornecer somente os recursos essenciais.	ec2- -check managedinstance-association-compliance-status	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-8(1)	A organização atualiza o inventári o dos component es do sistema de informações como parte integrante das instalações, remoções e atualizações do sistema de informaçõ es.	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-8(3)(a)	A organização: a. Emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-8(3)(a)	A organização: a. Emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2- -check managedinstance-association-compliance-status	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CM-8(3)(a)	A organização: a. Emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para detectar a presença de componentes de hardware, software e firmware não autorizados no sistema de informações	ec2- -check managedinstance-patch-compliance-status	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	elasticache-redis-cluster-automatic-verificação de backup	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-9(b)	A organização: b. Realiza backups das informações em nível de sistema contidas no sistema de informações [Atribuição: frequência definida pela organização consistente com os objetivos do tempo de recuperação e ponto de recuperação].	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	s3- bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperaç ão e a reconstit uição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elasticache-redis-cluster-automatic-verificação de backup	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	elb-cross-zone-load-balanceamento ativado	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
CP-10	A organização fornece a recuperação e a reconstituição do sistema de informações para um estado conhecido após uma interrupção, um comprometimento ou uma falha.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-2	O sistema de informações identifica e autentica de forma exclusiva os usuários organizacionais (ou processos que atuam em nome dos usuários organizacionais).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-2(1)(11)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (11) O sistema de informações implementa autenticação multifatorial para acesso remoto a contas privilegiadas e não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que está obtendo acesso e o dispositivo atenda [Atribuição: requisitos de força do mecanismo definidos pela organização].	root-account-hardware-mfa-habilitado	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-2(1)(11)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (11) O sistema de informações implementa autenticação multifatorial para acesso remoto a contas privilegiadas e não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que está obtendo acesso e o dispositivo atenda [Atribuição: requisitos de força do mecanismo definidos pela organização].	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-2(1)(2)(11)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas. (11) O sistema de informações implementa autenticação multifatorial para acesso remoto a contas privilegiadas e não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que está obtendo acesso e o dispositivo atenda [Atribuição: requisitos de força do mecanismo definidos pela organização].	mfa-enabled-for-iam-acesso ao console	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-2(1)(2)(11)	(1) O sistema de informações implementa a autenticação multifator para acesso à rede a contas privilegiadas. (2) O sistema de informações implementa a autenticação multifator para acesso à rede a contas não privilegiadas. (11) O sistema de informações implementa autenticação multifatorial para acesso remoto a contas privilegiadas e não privilegiadas, de modo que um dos fatores seja fornecido por um dispositivo separado do sistema que está obtendo acesso e o dispositivo atenda [Atribuição: requisitos de força do mecanismo definidos pela organização].	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-5(1)(a)(d)(e)	O sistema de informação, para autenticação baseada em senha: (a) Impõe a complexidade mínima da senha de [Atribuição: requisitos definidos pela organização para diferenciação de maiúsculas e minúsculas, número de caracteres, combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais, incluindo requisitos mínimos para cada tipo]; (d) Impõe restrições de vida útil mínima e máxima da senha de [Atribuição: números definidos pela organização para a vida útil mínima e a vida útil máxima]; (e) Proíbe a reutilização de senhas para gerações de [Atribuição: número definido pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-5(4)	A organização emprega ferrament as automatizadas para determina r se os autentica dores de senha são suficientemente fortes para satisfazer a [Atribuição: requisito s definidos pela organização].	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisito s estabelecidos pelo NIST SP 800-63 e pelo Centers for Internet Security (CIS) AWS Foundations Benchmark quanto à força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IA-5(7)	A organização garante que autenticadores estáticos não criptografados não sejam incorporados em aplicações ou scripts de acesso, nem armazenados em teclas de função.	codebuild-project-envvar-awscred-verificar	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IR-4(1)	A organização emprega mecanismos automatizados para oferecer suporte ao processo de tratamento de incidentes.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IR-6(1)	A organização emprega mecanismos automatizados para ajudar a comunicar incidentes de segurança.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
IR-7(1)	A organização emprega mecanismos automatizados para aumentar a disponibilidade de informações e suporte relacionados à resposta a incidentes.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
RA-5	A organização: a. Verifica vulnerabi lidades presentes no sistema de informaçõ es e nas aplicaçõe s hospedadas [Atribuição: frequênci a definida pela organização e/ou aleatoriamente, de acordo com o processo definido pela organização] e quando novas vulnerabilidades que potencialmente afetam o sistema ou aplicações são identificadas e reportadas; (b) Emprega ferramentas e técnicas de verificaç ão de vulnerabi lidades que facilitam a interoperabilidade entre ferrament as e automatizam partes do processo de gerenciamento de vulnerabilidades usando padrões para: 1. Enumerar plataformas, falhas de software e configura	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	ções impróprias; 2. Formatar listas de verificação e procedimentos de teste; e 3. Medir o impacto da vulnerabilidade; (c) Analisa relatórios de verificação de vulnerabilidade e resultados de avaliações de controle de segurança; (d) Corrige vulnerabilidades legítimas [Atribuição: tempos de resposta definidos pela organização], de acordo com uma avaliação organizacional de risco; e (e) Compartilha as informações obtidas no processo de verificação de vulnerabilidades e nas avaliações de controle de segurança com [Atribuição: pessoal ou perfis definidos pela organização] para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informações (ou		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	seja, fraquezas ou deficiências sistêmica s).		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
RA-5	A organização: a. Verifica vulnerabilidades presentes no sistema de informações e nas aplicações hospedadas [Atribuição: frequência definida pela organização e/ou aleatoriamente, de acordo com o processo definido pela organização] e quando novas vulnerabilidades que potencialmente afetam o sistema ou aplicações são identificadas e reportadas; (b) Emprega ferramentas e técnicas de verificação de vulnerabilidades que facilitam a interoperabilidade entre ferramentas e automatizam partes do processo de gerenciamento de vulnerabilidades usando padrões para: 1. Enumerar plataformas, falhas de software e configura	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	ções impróprias; 2. Formatar listas de verificação e procedimentos de teste; e 3. Medir o impacto da vulnerabilidade; (c) Analisa relatórios de verificação de vulnerabilidade e resultados de avaliações de controle de segurança; (d) Corrige vulnerabilidades legítimas [Atribuição: tempos de resposta definidos pela organização], de acordo com uma avaliação organizacional de risco; e (e) Compartilha as informações obtidas no processo de verificação de vulnerabilidades e nas avaliações de controle de segurança com [Atribuição: pessoal ou perfis definidos pela organização] para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informações (ou		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	seja, fraquezas ou deficiências sistêmicas).		
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	codebuild-project-envvar-awscred-verificar	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-3(a)	A organização: a. Gerencia o sistema de informações usando [Atribuição: ciclo de vida de desenvolvimento do sistema, definido pela organização] que incorpora questões de segurança das informações.	codebuild-project-source-repo-verificação de URL	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-10	A organização exige que o desenvolv edor do sistema de informações, do componente do sistema ou serviço do sistema de informaçõ es: (a) Execute o gerenciamento de configuração durante a [Seleção (uma ou mais): design; desenvolv imento; implement ação; operação]; do sistema, component e ou serviço. b. Documente, gerencie e controle a integrida de das alteraçõe s em [Atribuição: itens de configura ção definidos pela organização sob gerenciamento de configuração]; (c) Implement e somente as alterações aprovadas pela organizaç ão no sistema, no componente ou no serviço; (d) Documente as	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	alterações aprovadas no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-10	A organização exige que o desenvolvedor do sistema de informações, do componente do sistema ou serviço do sistema de informações: (a) Execute o gerenciamento de configuração durante a [Seleção (uma ou mais): design; desenvolvimento; implementação; operação]; do sistema, componente ou serviço. b. Documente, gerencie e controle a integridade das alterações em [Atribuição: itens de configuração definidos pela organização sob gerenciamento de configuração]; (c) Implemente somente as alterações aprovadas pela organização no sistema, no componente ou no serviço; (d) Documente as	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	alterações aprovadas no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-10	A organização exige que o desenvolv edor do sistema de informações, do componente do sistema ou serviço do sistema de informaçõ es: (a) Execute o gerenciamento de configuração durante a [Seleção (uma ou mais): design; desenvolv imento; implement ação; operação]; do sistema, component e ou serviço. b. Documente, gerencie e controle a integrida de das alteraçõe s em [Atribuição: itens de configura ção definidos pela organização sob gerenciamento de configuração]; (c) Implement e somente as alterações aprovadas pela organizaç ão no sistema, no componente ou no serviço; (d) Documente as	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	alterações aprovadas no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SA-10	A organização exige que o desenvolvedor do sistema de informações, do componente do sistema ou serviço do sistema de informações: (a) Execute o gerenciamento de configuração durante a [Seleção (uma ou mais): design; desenvolvimento; implementação; operação]; do sistema, componente ou serviço. b. Documente, gerencie e controle a integridade das alterações em [Atribuição: itens de configuração definidos pela organização sob gerenciamento de configuração]; (c) Implemente somente as alterações aprovadas pela organização no sistema, no componente ou no serviço; (d) Documente as	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	alterações aprovadas no sistema, no componente ou no serviço e os possíveis impactos de segurança das mudanças; e (e) Rastreie as falhas de segurança e a resolução de falhas no sistema, componente ou serviço e relate as descobertas para [Atribuição: pessoal definido pela organização].		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-group-has-users-verificar	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-2	O sistema de informações separa a funcionalidade do usuário (incluindo serviços de interface do usuário) da funcionalidade de gerenciamento do sistema de informações.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-4	O sistema de informações evita transferências não autorizadas e não intencionais de informações por meio de recursos compartil hados do sistema.	ec2- volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada . Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	autoscaling-group-elb-healthcheck-obrigatório	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	elb-cross-zone-load-balanceamento ativado	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-5	O sistema de informações protege ou limita os efeitos dos seguintes tipos de ataques de negação de serviço: [Atribuição: tipos de ataques de negação de serviço definidos pela organização ou referências a fontes dessas informações] empregando [Atribuição: proteções de segurança definidas pela organização].	rds-instance-deletion-protection-habilitado	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elb-tls-https-listeners-somente	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ec2- instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamen te; logicamente] separados das redes organizac ionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciad as que consistem em dispositivos de proteção de limites organizad os, de acordo com uma arquitetura de segurança organizac ional.	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	s3- bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	alb-http-drop-invalid-habilitado para cabeçalho	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7	O sistema de informações: (a) Monitora e controla as comunicações no limite externo do sistema e nos principais limites internos do sistema; (b) Implementa sub-redes para componentes do sistema acessíveis ao público que são [Seleção: fisicamente; logicamente] separados das redes organizacionais internas; e (c) Conecta-se a redes externas ou sistemas de informações somente por meio de interfaces gerenciadas que consistem em dispositivos de proteção de limites organizados, de acordo com uma arquitetura de segurança organizacional.	elasticsearch-node-to-node-verificação de criptografia	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	ec2- instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	internet-gateway-authorized-vpc-somente	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	ebs-snapshot-public-restorable-verificar	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	ec2- instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	lambda-function-public-access-proibido	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	rds-instance-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	redshift-cluster-public-access-verificar	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	blocos s3 account-level-public-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	s3- bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informações.	s3- bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	s3- bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	sagemaker-notebook-no-direct-acesso à internet	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	vpc-default-security-group-fechado	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-7(3)	A organização limita o número de conexões de rede externas ao sistema de informaçõ es.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	alb-http-drop-invalid-habilitado para cabeçalho	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	elasticsearch-node-to-node-verificação de criptografia	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	elb-tls-https-listeners-somente	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidencialidade; integridade] das informações transmitidas.	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8	O sistema de informações protege a [Seleção (uma ou mais): confidenc ialidade; integrida de] das informações transmitidas.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8(1)	O sistema de informações implementa mecanismos criptográ ficos para [Seleção (uma ou mais): impedir a divulgaçã o não autorizada de informações; detectar alteraçõe s nas informações] durante a transmiss ão, a menos que seja protegido de outra forma por [Atribuiç ão: proteções físicas alternativas definidas pela organização].	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	alb-http-drop-invalid-habilitado para cabeçalho	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elasticsearch-node-to-node-verificação de criptografia	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elb-tls-https-listeners-somente	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-8(1)	O sistema de informações implementa mecanismos criptográficos para [Seleção (uma ou mais): impedir a divulgação não autorizada de informações; detectar alterações nas informações] durante a transmissão, a menos que seja protegido de outra forma por [Atribuição: proteções físicas alternativas definidas pela organização].	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	cmk-backing-key-rotation-habilitado	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-12	A organização estabelece e gerencia as chaves criptográficas para atender aos critérios de criptografia necessários empregados no sistema de informações de acordo com [Atribuição: requisitos definidos pela organização para geração, distribuição, armazenamento, acesso e destruição de chaves].	kms-cmk-not-scheduled-para exclusão	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	api-gw-cache-enabl ede criptografado	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	habilitado para s3 bucket-server-side-encryption	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	s3- bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sagemaker-endpoint-configuration-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sagemaker-notebook-instance-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa [Atribuição: usos criptográficos definidos pela organização e tipo de criptografia necessária para cada uso] de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-13	O sistema de informações implementa criptografia validada pelo FIPS ou aprovada pela NSA, de acordo com as leis federais, ordens executivas, diretivas, políticas, regulamentos e padrões aplicáveis.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	alb-http-to-https-verificação de redirecionamento	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	alb-http-drop-invalid-habilitado para cabeçalho	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	O sistema de informações protege a autenticidade das sessões de comunicação.	elb-tls-https-listeners-somente	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	api-gw-cache-enabl ede criptografado	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidenc ialidade; integrida de] de [Atribuição: informações em repouso definidas pela organização].	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidenc ialidade; integrida de] de [Atribuição: informações em repouso definidas pela organização].	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidenc ialidade; integrida de] de [Atribuição: informações em repouso definidas pela organização].	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	kms-cmk-not-scheduled-para exclusão	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	s3- bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	habilitado para s3 bucket-server-side-encryption	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	sagemaker-endpoint-configuration-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	sagemaker-notebook-instance-kms-configurado por chave	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidenc ialidade; integrida de] de [Atribuição: informações em repouso definidas pela organização].	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidenc ialidade; integrida de] de [Atribuição: informações em repouso definidas pela organização].	ec2- ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	O sistema de informações protege a [Seleção (um ou mais): confidencialidade; integridade] de [Atribuição: informações em repouso definidas pela organização].	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SC-36	A organização distribui [Atribuição: processamento e armazenamento definidos pela organização] em vários locais físicos.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático

ID de controle	Descrição do controle	AWS Config Regra	Orientação
			no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SC-36	A organização distribui [Atribuição: processamento e armazenamento definidos pela organização] em vários locais físicos.	s3- bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-2(2)	A organização emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2- -check managedinstance-patch-compliance-status	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-2(2)	A organização emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-2(2)	A organização emprega mecanismos automatizados [Atribuição: frequência definida pela organização] para determinar o estado dos componentes do sistema de informações em relação à correção de falhas.	ec2- -check managedinstance-association-compliance-status	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(1)	A organização conecta e configura ferramentas individuais de detecção de intrusões em um sistema de detecção de intrusões que abrange todo o sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(2)	A organização emprega ferramentas automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-4(2)	A organização emprega ferrament as automatizadas para oferecer suporte à análise quase em tempo real dos eventos.	ec2- instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(4)	O sistema de informações monitora o tráfego de comunicações de entrada e saída [Atribuição: frequência definida pela organização] em busca de atividades ou condições incomuns ou não autorizadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(4)	O sistema de informações monitora o tráfego de comunicações de entrada e saída [Atribuição: frequência definida pela organização] em busca de atividades ou condições incomuns ou não autorizadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(4)	O sistema de informações monitora o tráfego de comunicações de entrada e saída [Atribuição: frequência definida pela organização] em busca de atividades ou condições incomuns ou não autorizadas.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(4)	O sistema de informações monitora o tráfego de comunicações de entrada e saída [Atribuição: frequência definida pela organização] em busca de atividades ou condições incomuns ou não autorizadas.	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicações de comprometimento ou possível comprometimento: [Atribuição: indicadores de comprometimento definidos pela organização].	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicaçõe s de compromet imento ou possível comprometimento: [Atribuição: indicador es de compromet imento definidos pela organização].	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicaçõe s de compromet imento ou possível comprometimento: [Atribuição: indicador es de compromet imento definidos pela organização].	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(5)	O sistema de informações alerta [Atribuição: pessoal ou funções definidas pela organização] quando ocorrem as seguintes indicações de comprometimento ou possível comprometimento: [Atribuição: indicadores de comprometimento definidos pela organização].	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(16)	A organização correlaciona as informações das ferramentas de monitoramento empregadas em todo o sistema de informações.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	guardduty-non-arch ived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classific ando as descobert as por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégi as e prioridades de correção. Essa regra permite que você defina opcionalm ente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	cloud-trail-cloud-watch-logs-habilitado	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-4(a)(b)(c)	A organização: a. Monitora o sistema de informações para detectar: 1. Ataques e indicadores de possíveis ataques de acordo com [Atribuição: objetivos de monitoramento definidos pela organização]; e 2. Conexões locais, de rede e remotas não autorizadas; (b) Identifica o uso não autorizado do sistema de informação por meio de [Atribuição: técnicas e métodos definidos pela organização]; (c) Implanta dispositivos de monitoramento: (i) estrategicamente dentro do sistema de informações para coletar informações essenciais determina das pela organizaç ão; e (ii) em locais ad hoc dentro do sistema para rastrear tipos específicos de transações de	ec2- instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
	interesse para a organização.		
SI-7	A organização emprega ferramentas de verificação de integridade para detectar alterações não autorizadas em [Atribuição: softwares, firmwares e informações definidos pela organização].	cloud-trail-log-file-habilitado para validação	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-7(1)	O sistema de informação realiza uma verificação de integridade de [Atribuição: software, firmware e informaçõ es definidos pela organização] [Seleção (uma ou mais): na inicialização; em [Atribuição: estados de transição definidos pela organização ou eventos relevantes para a segurança]; [Atribuição: frequênci a definida pela organização]].	ec2- -manager instance-managed-by-systems	É possível fazer um inventário das plataformas de software e aplicativos dentro da organizaç ão gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configura ções detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-7(1)	O sistema de informação realiza uma verificação de integridade de [Atribuição: software, firmware e informaçõ es definidos pela organização] [Seleção (uma ou mais): na inicialização; em [Atribuição: estados de transição definidos pela organização ou eventos relevantes para a segurança]; [Atribuição: frequênci a definida pela organização]].	ec2- -check managedinstance-pa tch-compliance-status	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-7(1)	O sistema de informação realiza uma verificação de integridade de [Atribuição: software, firmware e informações definidos pela organização] [Seleção (uma ou mais): na inicialização; em [Atribuição: estados de transição definidos pela organização ou eventos relevantes para a segurança]; [Atribuição: frequência definida pela organização]].	cloud-trail-log-file-habilitado para validação	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	s3- bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	elasticache-redis-cluster-automatic-verificação de backup	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informaçõ es dentro e fora do sistema de informaçõ es de acordo com as leis federais, ordens executivas, diretrizes, políticas , regulamentos, padrões e requisitos operacionais aplicávei s.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Config Regra	Orientação
SI-12	A organização lida e retém as informações dentro e fora do sistema de informações de acordo com as leis federais, ordens executivas, diretrizes, políticas, regulamentos, padrões e requisitos operacionais aplicáveis.	cw-loggroup-retention-period-verificar	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 800-53 rev 4.

Práticas recomendadas de operação do NIST 800-53 rev 5

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 800-53 e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles NIST 800-53. Um controle do NIST 800-53 pode estar relacionado a várias regras

de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			cliente não optou por privilégios elevados.
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AC-2(1)	Gerenciamento de contas | Gerenciamento automatizado de contas do sistema	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(3)	Gerenciamento de contas | Desabilitação de contas	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(3)	Gerenciamento de contas | Desabilitação de contas	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(3)	Gerenciamento de contas | Desabilitação de contas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatiz adas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatiz adas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatiz adas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(4)	Gerenciamento de contas | Ações de auditoria automatizadas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2(12)	Gerenciamento de contas | Monitoramento de contas para uso atípico	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-2	Gerenciamento de contas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-2	Gerenciamento de contas	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-3(7)	Fiscalização de acesso | Controle de acesso baseado em funções	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
AC-3(15)	Fiscalização de acesso | Controle de acesso discricionário e obrigatório	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-3	Fiscalização de acesso	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-3	Fiscalização de acesso	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
AC-3	Fiscalização de acesso	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-3	Fiscalização de acesso	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-3	Fiscalização de acesso	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-3	Fiscalização de acesso	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-3	Fiscalização de acesso	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-3	Fiscalização de acesso	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-3	Fiscalização de acesso	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-3	Fiscalização de acesso	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(21)	Fiscalização de fluxo de informações | Separação física ou lógica dos fluxos de informações	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4(26)	Fiscalização de fluxo de informações | Ações de filtragem de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
AC-4	Fiscalização de fluxo de informações	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-4	Fiscalização de fluxo de informações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
AC-4	Fiscalização de fluxo de informações	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
AC-4	Fiscalização de fluxo de informações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
AC-4	Fiscalização de fluxo de informações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4	Fiscalização de fluxo de informações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC-4	Fiscalização de fluxo de informações	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-4	Fiscalização de fluxo de informações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-4	Fiscalização de fluxo de informações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-4	Fiscalização de fluxo de informações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-4	Fiscalização de fluxo de informações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-4	Fiscalização de fluxo de informações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-4	Fiscalização de fluxo de informações	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5	Separação de deveres	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-5	Separação de deveres	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5	Separação de deveres	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5	Separação de deveres	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-5	Separação de deveres	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-5	Separação de deveres	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(2)	Privilégio mínimo | Acesso não privilegiado para funções não relacionadas à segurança	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(2)	Privilégio mínimo | Acesso não privilegiado para funções não relacionadas à segurança	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(2)	Privilégio mínimo | Acesso não privilegiado para funções não relacionadas à segurança	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegi ados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegi ados	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegi ados	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegi ados	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegiados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(3)	Privilégio mínimo | Acesso à rede para comandos privilegiados	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegiadas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(9)	Privilégio mínimo | Registo em log do uso de funções privilegi adas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(10)	Privilégio mínimo | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(10)	Privilégio mínimo | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6(10)	Privilégio mínimo | Proibição de usuários não privilegiados de executar funções privilegiadas	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
AC-6	Privilégio mínimo	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alteraçõe s nos metadados da instância.
AC-6	Privilégio mínimo	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
AC-6	Privilégio mínimo	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
AC-6	Privilégio mínimo	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-6	Privilégio mínimo	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
AC-6	Privilégio mínimo	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-6	Privilégio mínimo	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-6	Privilégio mínimo	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-6	Privilégio mínimo	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-6	Privilégio mínimo	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-6	Privilégio mínimo	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-17(2)	Acesso remoto | Proteção de confidencialidade e integridade usando criptografia	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
AC-21	Compartilhamento de informações	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
AC-21	Compartilhamento de informações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21	Compartilhamento de informações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
AC-21	Compartilhamento de informações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
AC-21	Compartilhamento de informações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
AC-21	Compartilhamento de informações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
AC-21	Compartilhamento de informações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AC-21	Compartilhamento de informações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
AC-21	Compartilhamento de informações	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-2	Registro em log de eventos	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-2	Registro em log de eventos	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-2	Registro em log de eventos	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-3	Conteúdo dos registros de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-3	Conteúdo dos registros de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-3	Conteúdo dos registros de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
AU-6(1)	Revisão, análise e geração de relatórios de registros de auditoria | Integração automatizada de processos	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)	Revisão, análise e geração de relatórios de registros de auditoria | Integração automatizada de processos	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)	Revisão, análise e geração de relatórios de registros de auditoria | Integração automatizada de processos	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(1)	Revisão, análise e geração de relatórios de registros de auditoria | Integração automatizada de processos	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatório s de auditoria | Correlação de repositórios de registros de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-6(3)	Revisão, análise e geração de relatório s de auditoria | Correlação de repositórios de registros de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatório s de auditoria | Correlação de repositórios de registros de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatório s de auditoria | Correlação de repositórios de registros de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(3)	Revisão, análise e geração de relatórios de auditoria | Correlação de repositórios de registros de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatório s de registros de auditoria | Revisão e análise central	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatório s de registros de auditoria | Revisão e análise central	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-6(4)	Revisão, análise e geração de relatório s de registros de auditoria | Revisão e análise central	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatório s de registros de auditoria | Revisão e análise central	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatório s de registros de auditoria | Revisão e análise central	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(4)	Revisão, análise e geração de relatórios de registros de auditoria | Revisão e análise central	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
AU-6(5)	Revisão, análise e geração de relatórios de registros de auditoria | Análise integrada de registros de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(5)	Revisão, análise e geração de relatórios de registros de auditoria | Análise integrada de registros de auditoria	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(5)	Revisão, análise e geração de relatório s de registros de auditoria | Análise integrada de registros de auditoria	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-6(5)	Revisão, análise e geração de relatórios de registros de auditoria | Análise integrada de registros de auditoria	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-7(1)	Redução de registros de auditoria e geração de relatório s | Processamento automático	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU-9(2)	Proteção de informações de auditoria | Armazenamento em sistemas ou componentes físicos separados	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9(2)	Proteção de informações de auditoria | Armazenamento em sistemas ou componentes físicos separados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9(2)	Proteção de informações de auditoria | Armazenamento em sistemas ou componentes físicos separados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9(7)	Proteção de informações de auditoria | Armazenamento em componente com sistema operacional diferente	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
AU-9	Proteção de informações de auditoria	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	Proteção de informações de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-9	Proteção de informações de auditoria	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	Proteção de informações de auditoria	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-9	Proteção de informações de auditoria	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
AU-10	Não repúdio	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-10	Não repúdio	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-10	Não repúdio	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-10	Não repúdio	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
AU-12	Geração de registros de auditoria	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
AU-12	Geração de registros de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-12	Geração de registros de auditoria	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
AU-14(1)	Auditoria de sessão | Inicialização do sistema	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
CA-7	Monitoramento contínuo	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
CA-7	Monitoramento contínuo	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificaç ões acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
CA-7	Monitoramento contínuo	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CA-7	Monitoramento contínuo	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-7	Monitoramento contínuo	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	rds-instance-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de sua(s) instância(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada . Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	redshift-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) do Amazon Redshift.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	sagemaker-endpoint -configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CA-9(1)	Conexões internas do sistema | Verificações de conformidade	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2(2)	Configuração de referência | Suporte de automação para precisão e moeda	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
CM-2	Configuração de referência	rds-instance-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de sua(s) instância(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	redshift-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) do Amazon Redshift.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-2	Configuração de referência	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3(6)	Controle de alteração de configuração | Gerenciamento de criptografia	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
CM-3	Controle de alteração de configuração	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-3	Controle de alteração de configuração	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7	Funcionalidade mínima	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
CM-7	Funcionalidade mínima	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-7	Funcionalidade mínima	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(1)	Inventário de componentes do sistema | Atualizações durante a instalação e a remoção	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(1)	Inventário de componentes do sistema | Atualizações durante a instalação e a remoção	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(2)	Inventário de componentes do sistema | Manutenção automatizada	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)	Inventário de componentes do sistema | Detecção automatizada de componentes não autorizados	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)	Inventário de componentes do sistema | Detecção automatizada de componentes não autorizados	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)	Inventário de componentes do sistema | Detecção automatizada de componentes não autorizados	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8(3)	Inventário de componentes do sistema | Detecção automatizada de componentes não autorizados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	Inventário de componentes do sistema	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CM-8	Inventário de componentes do sistema	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-2(2)	Plano de contingência | Planejamento de capacidade	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-2(2)	Plano de contingência | Planejamento de capacidade	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(1)	Local de armazenamento alternativo | Separação do local primário	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6(2)	Local de armazenamento alternativo | Objetivos de tempo de recuperação e ponto de recuperação	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-6	Local de armazenamento alternativo	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-9	Backup do sistema	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-9	Backup do sistema	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
CP-10	Recuperação e reconstituição do sistema	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
CP-10	Recuperação e reconstituição do sistema	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CP-10	Recuperação e reconstituição do sistema	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	Identificação e autenticação (usuários organizac ionais) | Autenticação multifator para contas privilegiadas	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	Identificação e autenticação (usuários organizac ionais) | Autenticação multifator para contas privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	Identificação e autenticação (usuários organizacionais) | Autenticação multifator para contas privilegiadas	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(1)	Identificação e autenticação (usuários organizacionais) | Autenticação multifator para contas privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(2)	Identificação e autenticação (usuários organizac ionais) | Autenticação multifator para contas não privilegiadas	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(2)	Identificação e autenticação (usuários organizac ionais) | Autenticação multifator para contas não privilegiadas	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(2)	Identificação e autenticação (usuários organizacionais) | Autenticação multifator para contas não privilegiadas	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(2)	Identificação e autenticação (usuários organizacionais) | Autenticação multifator para contas não privilegiadas	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(6)	Identificação e autenticação (usuários organizac ionais) | Acesso a contas: dispositivo separado	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(6)	Identificação e autenticação (usuários organizac ionais) | Acesso a contas: dispositivo separado	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(6)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: dispositivo separado	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(6)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: dispositivo separado	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(8)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: resistente à repetição	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(8)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: resistente à repetição	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(8)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: resistente à repetição	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-2(8)	Identificação e autenticação (usuários organizacionais) | Acesso a contas: resistente à repetição	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(1)	Gerenciamento de autenticadores | Autenticação baseada em senha	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IA-5(7)	Gerenciamento de autenticadores | Ausência de autenticadores estáticos não criptografados incorporados	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(1)	Tratamento de incidentes | Processos automatizados de tratamento de incidentes	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
IR-4(5)	Tratamento de incidentes | Desabilit ação automática do sistema	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RA-3(4)	Avaliação de risco | Análise cibernética preditiva	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3	Ciclo de vida de desenvolvimento do sistema	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-3	Ciclo de vida de desenvolvimento do sistema	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-8(19)	Princípios de engenharia de segurança e privacidade | Proteção contínua	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-8(21)	Princípios de engenharia de segurança e privacidade | Autoanálise	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-8(22)	Princípios de engenharia de segurança e privacidade | Responsabilidade e rastreabilidade	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-8(25)	Princípios de engenharia de segurança e privacidade | Segurança econômica	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-11(1)	Teste e avaliação de desenvolvedores | Análise de código estático	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-11(6)	Teste e avaliação de desenvolvedores | Avaliações da superfície de ataque	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-15(2)	Processo de desenvolvimento, padrões e ferramentas | Ferramentas de rastreamento de segurança e privacidade	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-15(2)	Processo de desenvolvimento, padrões e ferramentas | Ferramentas de rastreamento de segurança e privacidade	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-15(8)	Processo de desenvolvimento, padrões e ferramentas | Reutilização de informações sobre ameaças e vulnerabilidades	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SA-15(8)	Processo de desenvolvimento, padrões e ferramentas | Reutilização de informações sobre ameaças e vulnerabilidades	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(1)	enial-of-service Proteção D | Restringir a capacidade de atacar outros sistemas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(2)	enial-of-service Proteção D | Capacidade, largura de banda e redundância	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5(3)	enial-of-service Proteção D | Detecção e monitoramento	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-5	enial-of-service Proteção D	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SC-7(3)	Proteção de limites | Pontos de acesso	autoscaling-launch-config-public-ip-disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(3)	Proteção de limites | Pontos de acesso	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(3)	Proteção de limites | Pontos de acesso	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(3)	Proteção de limites | Pontos de acesso	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(3)	Proteção de limites | Pontos de acesso	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(3)	Proteção de limites | Pontos de acesso	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(3)	Proteção de limites | Pontos de acesso	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(3)	Proteção de limites | Pontos de acesso	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(3)	Proteção de limites | Pontos de acesso	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(4)	Proteção de limites | Serviços externos de telecomunicações	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(5)	Proteção de limites | Negação por padrão — Permissão por exceção	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(5)	Proteção de limites | Negação por padrão — Permissão por exceção	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(5)	Proteção de limites | Negação por padrão — Permissão por exceção	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(5)	Proteção de limites | Negação por padrão — Permissão por exceção	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(9)	Proteção de limites | Restrição do tráfego de comunicações de saída ameaçador	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
SC-7(10)	Proteção de limites | Prevenção de exfiltração	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC-7(10)	Proteção de limites | Prevenção de exfiltração	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
SC-7(10)	Proteção de limites | Prevenção de exfiltração	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
SC-7(10)	Proteção de limites | Prevenção de exfiltração	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
SC-7(10)	Proteção de limites | Prevenção de exfiltração	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(10)	Proteção de limites | Prevenção de exfiltração	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.
SC-7(10)	Proteção de limites | Prevenção de exfiltração	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(11)	Proteção de limites | Restringir o tráfego de comunicações de entrada	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(16)	Proteção de limites | Prevenção da descoberta de componentes do sistema	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(20)	Proteção de limites | Isolamento e segmentação dinâmicos	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7(21)	Proteção de limites | Isolamento de componentes do sistema	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
SC-7	Proteção de limites	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
SC-7	Proteção de limites	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7	Proteção de limites	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
SC-7	Proteção de limites	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
SC-7	Proteção de limites	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
SC-7	Proteção de limites	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
SC-7	Proteção de limites	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
SC-7	Proteção de limites	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-7	Proteção de limites	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(1)	Confidencialidade e integridade da transmissão | Proteção criptográfica	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8(2)	Confidencialidade e integridade da transmissão | Processamento antes e depois da transmissão	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	Confidencialidade e integridade da transmissão	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	Confidencialidade e integridade da transmissão	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8	Confidencialidade e integridade da transmissão	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	Confidencialidade e integridade da transmissão	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
SC-8	Confidencialidade e integridade da transmissão	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	Confidencialidade e integridade da transmissão	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-8	Confidencialidade e integridade da transmissão	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	Confidencialidade e integridade da transmissão	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-8	Confidencialidade e integridade da transmissão	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-8	Confidencialidade e integridade da transmissão	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-12(2)	Gerenciamento e estabelecimento de chaves criptográficas | Chaves simétricas	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12(2)	Gerenciamento e estabelecimento de chaves criptográficas | Chaves simétricas	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12(3)	Estabelecimento e gerenciamento de chaves criptográficas | Chaves assimétricas	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-12	Estabelecimento e gerenciamento de chaves criptográficas	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-12	Estabelecimento e gerenciamento de chaves criptográficas	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
SC-13	Proteção criptográfica	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
SC-13	Proteção criptográfica	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-13	Proteção criptográfica	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
SC-13	Proteção criptográfica	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-13	Proteção criptográfica	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	Proteção criptográfica	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC-13	Proteção criptográfica	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	Proteção criptográfica	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
SC-13	Proteção criptográfica	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
SC-13	Proteção criptográfica	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-13	Proteção criptográfica	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC-13	Proteção criptográfica	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
SC-13	Proteção criptográfica	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SC-13	Proteção criptográfica	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
SC-13	Proteção criptográfica	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-13	Proteção criptográfica	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(3)	Autenticidade da sessão | Identificadores de sessão exclusivos gerados pelo sistema	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
SC-23(3)	Autenticidade da sessão | Identificadores de sessão exclusivos gerados pelo sistema	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-23(3)	Autenticidade da sessão | Identific adores de sessão exclusivos gerados pelo sistema	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(3)	Autenticidade da sessão | Identificadores de sessão exclusivos gerados pelo sistema	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23(5)	Autenticidade da sessão | Autoridades de certificação permitidas	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23(5)	Autenticidade da sessão | Autoridades de certificação permitidas	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	Autenticidade da sessão	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	Autenticidade da sessão	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	Autenticidade da sessão	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
SC-23	Autenticidade da sessão	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	Autenticidade da sessão	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	Autenticidade da sessão	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	Autenticidade da sessão	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SC-23	Autenticidade da sessão	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-23	Autenticidade da sessão	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SC-23	Autenticidade da sessão	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(1)	Proteção de informações em repouso | Proteção criptográfica	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28(3)	Proteção de informações em repouso | Chaves criptográficas	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
SC-28(3)	Proteção de informações em repouso | Chaves criptográficas	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
SC-28	Proteção de informações em repouso	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	Proteção de informações em repouso	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
SC-28	Proteção de informações em repouso	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	Proteção de informações em repouso	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SC-28	Proteção de informações em repouso	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
SC-28	Proteção de informações em repouso	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
SC-28	Proteção de informações em repouso	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SC-28	Proteção de informações em repouso	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
SC-28	Proteção de informações em repouso	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SC-28	Proteção de informações em repouso	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-28	Proteção de informações em repouso	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-36(2)	Processamento e armazenamento distribuídos | Sincronização	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-36	Processamento e armazenamento distribuídos	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-36	Processamento e armazenamento distribuídos	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-36	Processamento e armazenamento distribuídos	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SC-36	Processamento e armazenamento distribuídos	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	Remediação de falhas | Status automatizado de remediação de falhas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	Remediação de falhas | Status automatizado de remediação de falhas	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(2)	Remediação de falhas | Status automatizado de remediação de falhas	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(3)	Remediação de falhas | Tempo para remediação de falhas e benchmarks para ações corretivas	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(3)	Remediação de falhas | Tempo para remediação de falhas e benchmarks para ações corretivas	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(3)	Remediação de falhas | Tempo para remediação de falhas e benchmarks para ações corretivas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(4)	Remediação de falhas | Ferramentas automatizadas de gerenciamento de patches	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(4)	Remediação de falhas | Ferramentas automatizadas de gerenciamento de patches	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(4)	Remediação de falhas | Ferramentas automatizadas de gerenciamento de patches	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(5)	Remediação de falhas | Atualizações automáticas de software e firmware	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(5)	Remediação de falhas | Atualizações automáticas de software e firmware	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2(5)	Remediação de falhas | Atualizações automáticas de software e firmware	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
SI-2	Remediação de falhas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-2	Remediação de falhas	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificações acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-3(8)	Proteção contra códigos mal-intencionados | Detecção de comandos não autorizados	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(1)	Monitoramento de sistemas | Sistema de detecção de invasões em todo o sistema	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(2)	Monitoramento de sistemas | Ferramentas e mecanismos automatizados para análise em tempo real	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SI-4(4)	Monitoramento de sistemas | Tráfego de comunicações de entrada e saída	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificaç ões acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(4)	Monitoramento de sistemas | Tráfego de comunicações de entrada e saída	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	Monitoramento de sistemas | Alertas gerados pelo sistema	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(5)	Monitoramento de sistemas | Alertas gerados pelo sistema	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-4(5)	Monitoramento de sistemas | Alertas gerados pelo sistema	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(12)	Monitoramento de sistemas | Alertas automatizados gerados pela organização	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(13)	Monitoramento de sistemas | Análise de padrões de tráfego e de eventos	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(20)	Monitoramento de sistemas | Usuários privilegiados	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(22)	Monitoramento de sistemas | Serviços de rede não autorizados	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4(25)	Monitoramento de sistemas | Otimização da análise do tráfego de rede	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
SI-4	Monitoramento de sistemas	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificaç ões acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	Monitoramento de sistemas	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-4	Monitoramento de sistemas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(1)	Integridade de software, firmware e informações | Verificações de integridade	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(3)	Integridade de software, firmware e informações | Ferramentas de integridade gerenciadas centralmente	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(6)	Integridade de software, firmware e informações | Proteção criptográfica	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(7)	Integridade de software, firmware e informações | Integração de detecção e resposta	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-7(8)	Integridade de software, firmware e informações | Capacidade de auditoria para eventos significativos	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informaçõ es	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informações	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informações	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informações	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informaçõ es	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informações	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-12	Gerenciamento e retenção de informações	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	s3-version-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-13(5)	Prevenção previsível de falhas | Capacidade de failover	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-20	Aplicação de taint	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
SI-20	Aplicação de taint	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
SI-20	Aplicação de taint	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 800-53 rev 5.

Práticas recomendadas operacionais do NIST 800 171

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 800-171 e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles NIST 800-171. Um controle do NIST 800-171 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizados e dispositivos (incluindo outros sistemas).	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.1	Limite o acesso de usuários autorizados ao sistema, processos que atuam em nome de usuários autorizad os e dispositivos (incluindo outros sistemas).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	internet-gateway-a uthorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.1.2	Limite o acesso ao sistema para os tipos de transações e funções que os usuários autorizados têm permissão para executar.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.2	Limite o acesso ao sistema para os tipos de transaçõe s e funções que os usuários autorizados têm permissão para executar.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3	Controle o fluxo de CUI de acordo com as autorizações aprovadas.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-inten cionadas sem conluio.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.4	Separe os deveres dos indivíduos para reduzir o risco de atividades mal-intencionadas sem conluio.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.5	Empregue o princípio de privilégio mínimo, inclusive para contas privilegiadas e funções de segurança específicas.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.6	Use contas ou perfis não privilegiados ao acessar funções não relacionadas à segurança.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.7	Impeça que usuários sem privilégios executem funções privilegiadas e audite a execução de tais funções.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.1.12	Monitore e controle as sessões de acesso remoto.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.12	Monitore e controle as sessões de acesso remoto.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.13	Empregue mecanismos criptográficos para proteger a confidencialidade das sessões de acesso remoto.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.14	Roteie o acesso remoto por meio de pontos de controle de acesso gerenciado.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.20	Verifique e controle/limite as conexões aos sistemas externos e o uso deles.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoramento, a análise, a investigação e o relato de atividades ilegais, não autorizadas ou inadequadas do sistema.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.1	Crie e retenha registros de auditoria do sistema na medida do necessário para permitir o monitoram ento, a análise, a investigação e o relato de atividades ilegais, não autorizad as ou inadequadas do sistema.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individuais do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.2	Garanta que as ações de usuários individua is do sistema possam ser rastreadas para que eles possam ser responsabilizados por suas ações.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.4	Alerta em caso de falha no processo de uma auditoria.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.4	Alerta em caso de falha no processo de uma auditoria.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.5	Correlacione processos de revisão, análise e relatório de auditoria para investigação e resposta a indícios de atividades inadequadas, suspeitas ou incomuns.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.5	Correlacione processos de revisão, análise e relatório de auditoria para investigação e resposta a indícios de atividades inadequadas, suspeitas ou incomuns.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3.8	Proteja as informações de auditoria e as ferramentas de auditoria contra acessos, modificações e exclusões não autorizados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.1	Estabeleça e mantenha inventários e configurações de linha de base de sistemas organizacionais (incluindo hardware, software, firmware e documentação) durante os respectivos ciclos de vida de desenvolvimento do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorad os para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multiloca ção de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.4.6	O princípio da funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.7	Restrinja, desabilit e e impeça o uso de funções, portas, protocolos ou serviços não essenciais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.7	Restrinja, desabilit e e impeça o uso de funções, portas, protocolos ou serviços não essenciais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.7	Restrinja, desabilit e e impeça o uso de funções, portas, protocolos ou serviços não essenciais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.7	Restrinja, desabilit e e impeça o uso de funções, portas, protocolos ou serviços não essenciais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.9	Controle e monitore softwares instalados pelo usuário.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.9	Controle e monitore softwares instalados pelo usuário.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas organizacionais.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas organizacionais.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2	Autentique (ou verifique) as identidades desses usuários, processos ou dispositivos como um pré-requisito para permitir o acesso aos sistemas organizacionais.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Use a autenticação multifator para acesso local e de rede a contas privilegiadas e para acesso de rede a contas não privilegi adas.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.5	Evite a reutilização de identificadores por um período definido.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.6	Desabilite os identificadores após um período definido de inatividade.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.7	Aplique uma alteração e caracteres e uma complexidade mínima de senha quando novas senhas forem criadas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.8	Proíba a reutilização de senhas por um número especificado de gerações.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.10	Armazene e transmita somente senhas protegidas por criptografia.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1	Estabeleça um recurso operacion al de tratament o de incidente s para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção , recuperação e resposta do usuário.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.1	Estabeleça um recurso operacional de tratamento de incidentes para sistemas organizacionais que inclua atividades de preparação, detecção, análise, contenção, recuperação e resposta do usuário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11.2	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam o sistema são identificadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11.2	Verifique se há vulnerabilidades em sistemas e aplicaçõe s organizacionais periodicamente e quando novas vulnerabilidades que afetam o sistema são identificadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11.3	Corrija vulnerabilidades de acordo com avaliações de risco.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.1	Monitore, controle e proteja as comunicações (ou seja, informações transmitidas ou recebidas pelos sistemas organizacionais) nas fronteiras externas e nas principais fronteiras internas dos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolv imento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizac ionais.	ebs-optimized-inst ance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimizaçã o proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/ S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.2	Utilize projetos arquitetônicos, técnicas de desenvolvimento de software e princípios de engenharia de sistemas que promovam a segurança efetiva das informações nos sistemas organizacionais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.6	Por padrão, negue o tráfego de comunicações de rede e permita o tráfego de comunicações de rede por exceção (ou seja, negue tudo, permita por exceção).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.6	Por padrão, negue o tráfego de comunicações de rede e permita o tráfego de comunicações de rede por exceção (ou seja, negue tudo, permita por exceção).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.6	Por padrão, negue o tráfego de comunicações de rede e permita o tráfego de comunicações de rede por exceção (ou seja, negue tudo, permita por exceção).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.13.8	Implemente mecanismos criptográficos para evitar a divulgação não autorizada de CUI durante a transmissão, a menos que ela seja protegida de maneira física.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.13.10	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas depois de atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.10	Estabeleça e gerencie chaves criptográficas para criptografia usada em sistemas organizacionais.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
3.13.16	Proteja a confidencialidade de CUI em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
3.13.16	Proteja a confidencialidade de CUI em repouso.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptografia em repouso para ajudar a protegê-los.
3.13.16	Proteja a confidencialidade de CUI em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
3.13.16	Proteja a confidencialidade de CUI em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
3.13.16	Proteja a confidencialidade de CUI em repouso.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidencialidade de CUI em repouso.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
3.13.16	Proteja a confidenc ialidade de CUI em repouso.	sagemaker-endpoint -configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.1	Identifique, relate e corrija falhas do sistema de informaçõ es em tempo hábil.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.1	Identifique, relate e corrija falhas do sistema de informações em tempo hábil.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2	Forneça proteção contra códigos maliciosos em locais apropriados nos sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.3	Monitore alertas e recomendações de segurança do sistema e tome providências em resposta a eles.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.4	Atualize os mecanismos de proteção contra códigos malicioso s quando novas versões estiverem disponíveis.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6	Monitore sistemas organizacionais, incluindo tráfego de comunicações de entrada e saída, para detectar ataques e indicadores de possíveis ataques.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearc h Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizacionais.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7	Identifique o uso não autorizado de sistemas organizac ionais.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 800 171.

Práticas recomendadas operacionais do NIST 800 172

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 800-172 e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou

mais controles NIST 800-172. Um controle do NIST 800-172 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.		para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	ec2-instance-no-pu blic-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	autoscaling-launch -config-public-ip-disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informações entre domínios de segurança em sistemas conectados.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informações entre domínios de segurança em sistemas conectados.	clb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	ec2-token-hop-limit-check	A resposta HTTP PUT do serviço de metadados de instância (IMDS) deve ser restrita à instância do Amazon Elastic Compute Cloud (Amazon EC2). Com o IMDSv2, a resposta PUT que contém o token secreto por padrão não pode sair da instância, porque o limite de salto de resposta de metadados está definido como 1 (padrão do Config). Se esse valor for maior que 1, o token poderá sair da instância do EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1.3e	Use [Atribuição: soluções seguras de transferência de informações definidas pela organização] para controlar os fluxos de informaçõ es entre domínios de segurança em sistemas conectados.	nacl-no-unrestricted-ssh-rdp	As portas de administr ação do servidor remoto em suas listas de controle de acesso à rede (ACL da rede), como a porta 22 (SSH) e a porta 3389 (RDP), não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional a recursos na VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.2.1e	Ofereça treinamento de conscientização [Atribuição: frequência definida pela organização] com foco em reconhecer e responder a ameaças de engenharia social, agentes avançados de ameaças persistentes, violações e comportamentos suspeitos; atualize o treinamento [Atribuição: frequência definida pela organização] ou quando houver alterações significativas na ameaça.	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.2e	Use mecanismos automatizados para detectar componentes do sistema mal configurados ou não autorizados; após a detecção, [Seleção (um ou mais): remover os componentes; colocar os componentes em uma rede de quarentena ou remediação] para facilitar a aplicação de patches, a reconfiguração ou outras mitigações.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.2e	Use mecanismos automatizados para detectar componentes do sistema mal configurados ou não autorizados; após a detecção, [Seleção (um ou mais): remover os componentes; colocar os componentes em uma rede de quarentena ou remediação] para facilitar a aplicação de patches, a reconfiguração ou outras mitigações.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.2e	Use mecanismos automatizados para detectar componentes do sistema mal configurados ou não autorizados; após a detecção, [Seleção (um ou mais): remover os componentes; colocar os componentes em uma rede de quarentena ou remediação] para facilitar a aplicação de patches, a reconfiguração ou outras mitigações.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.2e	Use mecanismos automatizados para detectar componentes do sistema mal configurados ou não autorizados; após a detecção, [Seleção (um ou mais): remover os componentes; colocar os componentes em uma rede de quarentena ou remediação] para facilitar a aplicação de patches, a reconfiguração ou outras mitigações.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.3e	Empregue ferramentas automatizadas de descoberta e gerenciamento para manter um inventário completo up-to-date, preciso e prontamente disponível dos componentes do sistema.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.3e	Empregue ferramentas automatizadas de descoberta e gerenciamento para manter um inventário completo up-to-date, preciso e prontamente disponível dos componentes do sistema.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.3e	Empregue ferramentas automatizadas de descoberta e gerenciamento para manter um inventário completo up-to-date, preciso e prontamente disponível dos componentes do sistema.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4.3e	Empregue ferramentas automatizadas de descoberta e gerenciamento para manter um inventário completo up-to-date, preciso e prontamente disponível dos componentes do sistema.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.
3.4.3e	Empregue ferramentas automatizadas de descoberta e gerenciamento para manter um inventário completo up-to-date, preciso e prontamente disponível dos componentes do sistema.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2e	Use mecanismos automatizados para a geração, proteção, alternância e gerenciamento de senhas para sistemas e componentes do sistema que não oferecem suporte à autenticação multifator ou ao gerenciamento complexo de contas.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2e	Use mecanismos automatizados para a geração, proteção, alternância e gerenciamento de senhas para sistemas e componentes do sistema que não oferecem suporte à autenticação multifator ou ao gerenciamento complexo de contas.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
3.5.2e	Use mecanismos automatizados para a geração, proteção, alternância e gerenciamento de senhas para sistemas e componentes do sistema que não oferecem suporte à autenticação multifator ou ao gerenciamento complexo de contas.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2e	Use mecanismos automatizados para a geração, proteção, alternância e gerenciamento de senhas para sistemas e componentes do sistema que não oferecem suporte à autenticação multifator ou ao gerenciamento complexo de contas.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11.1e	Use [Tarefa: fontes de inteligência contra ameaças definidas pela organizaç ão] como parte de uma avaliação de risco para orientar e informar o desenvolv imento de sistemas organizacionais, arquiteturas de segurança, seleção de soluções de segurança, monitoram ento, busca de ameaças e atividade s de resposta e recuperação.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.11.2e	Conduza atividades de busca de ameaças cibernéticas [Seleção (uma ou mais): [Atribuição: frequência definida pela organização]; [Atribuição: evento definido pela organização]] para pesquisar indicadores de comprometimento em [Atribuição: sistemas definidos pela organização] e detectar, rastrear e interromper ameaças que escapam aos controles existentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
3.11.5e	Avalie a eficácia das soluções de segurança [Atribuição: frequência definida pela organização] para lidar com o risco previsto para os sistemas organizacionais e para a organização com base na inteligência contra ameaças atual e acumulada.	annual-risk-assessment-performed (verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	nacl-no-unrestricted-ssh-rdp	As portas de administração do servidor remoto em suas listas de controle de acesso à rede (ACL da rede), como a porta 22 (SSH) e a porta 3389 (RDP), não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional a recursos na VPC.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.13.4e	Use [Seleção: (uma ou mais): [Atribuição: técnicas de isolamento físico definidas pela organização]; [Atribuição: técnicas de isolamento lógico definidas pela organização]] em sistemas organizacionais e componentes do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.1e	Verifique a integrida de de [Atribuição: software essencial ou essencial de segurança definido pela organização] usando mecanismos de raiz de confiança ou assinaturas criptográficas.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuam ente os sistemas organizacionais e os component es do sistema em busca de comportam entos anômalos ou suspeitos.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
3.14.2e	Monitore continuam ente os sistemas organizacionais e os component es do sistema em busca de comportam entos anômalos ou suspeitos.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuam ente os sistemas organizacionais e os component es do sistema em busca de comportam entos anômalos ou suspeitos.	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuamente os sistemas organizacionais e os componentes do sistema em busca de comportamentos anômalos ou suspeitos.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuamente os sistemas organizacionais e os componentes do sistema em busca de comportamentos anômalos ou suspeitos.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuamente os sistemas organizacionais e os componentes do sistema em busca de comportamentos anômalos ou suspeitos.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.2e	Monitore continuam ente os sistemas organizacionais e os component es do sistema em busca de comportam entos anômalos ou suspeitos.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector , Amazon Macie AWS , Identity and Access Managemen t (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.6e	Use informaçõ es de indicador es de ameaças e mitigações efetivas obtidas de [Atribuiç ão: organizações externas definidas pela organizaç ão] para orientar e informar a detecção de intrusões e a busca de ameaças.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7e	Verifique a exatidão de [Atribuição: componentes essenciais de software, firmware e hardware de segurança definidos pela organização] usando [Atribuição: métodos ou técnicas de verificação definidos pela organização].	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7e	Verifique a exatidão de [Atribuição: componentes essenciais de software, firmware e hardware de segurança definidos pela organização] usando [Atribuição: métodos ou técnicas de verificação definidos pela organização].	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7e	Verifique a exatidão de [Atribuição: componentes essenciais de software, firmware e hardware de segurança definidos pela organização] usando [Atribuição: métodos ou técnicas de verificação definidos pela organização].	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7e	Verifique a exatidão de [Atribuição: componentes essenciais de software, firmware e hardware de segurança definidos pela organização] usando [Atribuição: métodos ou técnicas de verificação definidos pela organização].	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrado um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataforma. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataforma.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.14.7e	Verifique a exatidão de [Atribuição: componentes essenciais de software, firmware e hardware de segurança definidos pela organização] usando [Atribuição: métodos ou técnicas de verificação definidos pela organização].	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 800 172.

Práticas recomendadas operacionais do NIST 800 181

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 800 181 e as regras gerenciadas AWS do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um

ou mais controles do NIST 800 181. Um controle do NIST 800 181 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0008	Analise e planeje as mudanças previstas nos requisitos de capacidade de dados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	opensearch-encrypted-at-rest	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os domínios do Amazon Elasticsearch Service (Amazon ES).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisito s de confidenc ialidade, integridade e disponibilidade da organização.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0017	Aplique princípios de arquitetura de segurança orientada a serviços para atender aos requisitos de confidencialidade, integridade e disponibilidade da organização.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0024	Colete e mantenha os dados necessários para atender aos relatórios de segurança cibernética do sistema.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0042	Coordene com analistas de defesa cibernética para gerenciar e administrar a atualização de regras e assinaturas (por exemplo, sistemas de detecção/proteção de intrusões, antivírus e listas negras de conteúdo) para aplicativos especializados de defesa cibernética.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0047	Correlacione dados de incidentes para identificar vulnerabilidades específicas e fazer recomendações que permitam uma correção rápida.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	backup-recovery-po int-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	dynamodb-autoscali ng-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidad e de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidad e provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	dynamodb-throughpu t-limit-check	Habilite essa regra para garantir que a capacidade de throughput provision ada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidad e de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalm ente os parâmetro s AccountRCU ThresholdPercentag e (Config Default: 80) e AccountWCU ThresholdPercentag e (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	backup-plan-min-fr equency-and-min-re tention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyV alue parâmetros (Config default: 1), (requiredRetentionD aysConfig default: 35) e (requiredF requencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0051	Defina os níveis adequados de disponibilidade do sistema com base nas funções críticas do sistema e garanta que os requisitos do sistema identifiq uem os requisito s adequados de recuperação de desastres e continuid ade das operações, incluindo quaisquer requisitos adequados de local alternativo ou de failover, requisito s de backup e requisitos de suporte de material para recuperação/restau ração do sistema.	ec2-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0065	Desenvolva e implemente procedimentos de backup e recuperação de rede.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0070	Desenvolva planos de recuperação de desastres e continuidade de operações para sistemas em desenvolvimento e garanta testes antes que os sistemas entrem em um ambiente de produção.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0086	Garanta que a aplicação de patches de segurança para produtos comerciais integrados ao design do sistema atenda aos cronogramas ditados pela autoridade de gerenciamento para o ambiente operacional pretendido.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0086	Garanta que a aplicação de patches de segurança para produtos comerciais integrados ao design do sistema atenda aos cronogramas ditados pela autoridade de gerenciamento para o ambiente operacional pretendido.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0086	Garanta que a aplicação de patches de segurança para produtos comerciais integrados ao design do sistema atenda aos cronogramas ditados pela autoridade de gerenciamento para o ambiente operacional pretendido.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0086	Garanta que a aplicação de patches de segurança para produtos comerciais integrados ao design do sistema atenda aos cronogramas ditados pela autoridade de gerenciamento para o ambiente operacional pretendido.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0110	Identifique e/ou determine se um incidente de segurança é indicativo de uma violação da lei que requer ação legal específica.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0110	Identifique e/ou determine se um incidente de segurança é indicativo de uma violação da lei que requer ação legal específica.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0110	Identifique e/ou determine se um incidente de segurança é indicativo de uma violação da lei que requer ação legal específica.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0128	Integre recursos automatizados para atualização ou aplicação de patches no software do sistema sempre que possível e desenvolva processos e procedimentos para atualização e aplicação de patches manuais no software do sistema com base nos requisitos atuais e projetados do cronograma de patches para o ambiente operacional do sistema.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0128	Integre recursos automatizados para atualização ou aplicação de patches no software do sistema sempre que possível e desenvolva processos e procedimentos para atualização e aplicação de patches manuais no software do sistema com base nos requisito s atuais e projetado s do cronograma de patches para o ambiente operacional do sistema.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0128	Integre recursos automatizados para atualização ou aplicação de patches no software do sistema sempre que possível e desenvolva processos e procedimentos para atualização e aplicação de patches manuais no software do sistema com base nos requisitos atuais e projetados do cronograma de patches para o ambiente operacional do sistema.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0128	Integre recursos automatizados para atualização ou aplicação de patches no software do sistema sempre que possível e desenvolva processos e procedimentos para atualização e aplicação de patches manuais no software do sistema com base nos requisitos atuais e projetados do cronograma de patches para o ambiente operacional do sistema.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais dentro do

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			realm, as senhas e outras informações administrativas sobre cada entidade.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticsearch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicação segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositivo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0144	Gerencie contas, direitos de rede e acesso a sistemas e equipamentos.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0151	Monitore e avalie a eficácia das proteções de segurança cibernética da empresa para garantir que elas forneçam o nível de proteção pretendido.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0151	Monitore e avalie a eficácia das proteções de segurança cibernética da empresa para garantir que elas forneçam o nível de proteção pretendido.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0151	Monitore e avalie a eficácia das proteções de segurança cibernética da empresa para garantir que elas forneçam o nível de proteção pretendido.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-automatic-mino r-version-upgrade-enabled	Habilite atualizaç ões automáticas de versões secundári as nas instâncias do Amazon Relationa l Database Service (RDS) para garantir que as últimas atualizações de versões secundári as do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.
T0152	Monitore e mantenha bancos de dados para garantir o desempenho ideal.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0152	Monitore e mantenha bancos de dados para garantir o desempenh o ideal.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0153	Monitore a capacidade e o desempenho da rede.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0153	Monitore a capacidade e o desempenho da rede.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0153	Monitore a capacidad e e o desempenho da rede.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0153	Monitore a capacidade e o desempenho da rede.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0154	Monitore e relate o uso de ativos e recursos de gerenciamento de conhecimento.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0156	Supervisione e faça recomendações sobre o gerenciamento de configurações.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0160	Aplique patches nas vulnerabilidades da rede para garantir que as informações sejam protegidas contra terceiros.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0160	Aplique patches nas vulnerabilidades da rede para garantir que as informações sejam protegidas contra terceiros.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0160	Aplique patches nas vulnerabilidades da rede para garantir que as informações sejam protegidas contra terceiros.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0162	Execute backup e recuperação de bancos de dados para garantir a integridade dos dados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	cw-loggroup-retent ion-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelm ente mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlação de eventos usando informações coletadas de várias fontes na empresa para obter consciência situacional e determinar a eficácia de um ataque observado.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlação de eventos usando informações coletadas de várias fontes na empresa para obter consciência situacional e determinar a eficácia de um ataque observado.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0166	Realize a correlaçã o de eventos usando informaçõ es coletadas de várias fontes na empresa para obter consciência situacion al e determinar a eficácia de um ataque observado.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0168	Execute a comparaçã o de hash com o banco de dados estabelecido.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticse arch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicaç ão segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositi vo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0195	Forneça um fluxo gerenciado de informações relevantes (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0195	Forneça um fluxo gerenciado de informações relevante s (por meio de portais baseados na web ou outros meios) com base nos requisitos da missão.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0215	Reconheça uma possível violação de segurança e tome as medidas apropriad as para denunciar o incidente, conforme necessário.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0244	Verifique se as posturas de segurança do software/rede/sistema da aplicação estão implementadas conforme declarado, documente os desvios e recomende as ações necessárias para corrigir esses desvios.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0244	Verifique se as posturas de segurança do software/rede/sistema da aplicação estão implementadas conforme declarado, documente os desvios e recomende as ações necessárias para corrigir esses desvios.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0244	Verifique se as posturas de segurança do software/rede/sistema da aplicação estão implementadas conforme declarado, documente os desvios e recomende as ações necessárias para corrigir esses desvios.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0258	Forneça recursos de detecção, identificação e alerta oportunos sobre possíveis ataques/invasões, atividades anômalas e atividades de uso indevido e diferenci e esses incidentes e eventos de atividades benignas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0259	Use ferramentas de defesa cibernética para monitoramento e análise contínuos da atividade do sistema para identificar atividades mal-intencionadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticsearch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicação segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositivo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0262	Empregue defense-in-depth princípios e práticas aprovados (por exemplo, defense-in-multiple locais, defesas em camadas, robustez de segurança).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	autoscaling-launch -config-public-ip- disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	ec2-instance-profile- attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	s3-account-level-p ublic-access-blocks- periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticse arch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicaç ão segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositi vo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0284	Projete e desenvolva novas ferramentas/tecnologias relacionadas à segurança cibernética.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0284	Projete e desenvolv a novas ferramentas/ tecnologias relaciona das à segurança cibernética.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0306	Compatível com gerenciamento de incidentes, gerenciamento de níveis de serviço, gerenciamento de mudanças, gerenciamento de versões, gerenciamento de continuidade e gerenciamento de disponibilidade para bancos de dados e sistemas de gerenciamento de dados.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0306	Compatível com gerenciamento de incidentes, gerenciamento de níveis de serviço, gerenciamento de mudanças, gerenciamento de versões, gerenciamento de continuidade e gerenciamento de disponibilidade para bancos de dados e sistemas de gerenciamento de dados.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0306	Compatível com gerenciamento de incidentes, gerenciamento de níveis de serviço, gerenciamento de mudanças, gerenciamento de versões, gerenciamento de continuidade e gerenciamento de disponibilidade para bancos de dados e sistemas de gerenciamento de dados.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0314	Desenvolva um contexto de segurança do sistema, um Conceito de Operações (CONOPS) preliminar de segurança do sistema e defina os requisitos básicos de segurança do sistema de acordo com os requisitos de segurança cibernética aplicáveis.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0333	Realize análises e relatórios de tendências de defesa cibernética.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0333	Realize análises e relatórios de tendências de defesa cibernética.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0347	Avalie a validade dos dados de origem e das descobertas subsequentes.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolv a a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegi ado.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolva a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegiado.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolv a a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegi ado.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0358	Projete e desenvolv a a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegi ado.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolv a a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegi ado.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0358	Projete e desenvolva a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegiado.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolva a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegiado.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0358	Projete e desenvolv a a funcionalidade de administração e gerenciamento do sistema para usuários com acesso privilegi ado.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implemente e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizacionais.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0376	Estabeleça, forneça recursos, implemente e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizacionais.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implemente e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizacionais.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0376	Estabeleça, forneça recursos, implement e e avalie programas cibernéticos de gerenciamento da força de trabalho de acordo com os requisitos organizac ionais.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existentes de infraestrutura de chave pública (PKI) e incorporando funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existentes de infraestrutura de chave pública (PKI) e incorporando funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existentes de infraestrutura de chave pública (PKI) e incorporando funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0416	Habilite aplicações com chave pública aproveitando as bibliotecas existente s de infraestrutura de chave pública (PKI) e incorpora ndo funcionalidades de gerenciamento e criptografia de certificados quando apropriado.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	autoscaling-launch -config-public-ip-disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecimento organizacional explícito (por exemplo, documentos impressos, arquivos digitais).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0421	Gerencie a indexação /catalogação, o armazenamento e o acesso ao conhecime nto organizac ional explícito (por exemplo, documento s impressos, arquivos digitais).	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticse arch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicaç ão segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositi vo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégi o mínimo e. need-to-k now	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0475	Avalie os controles de acesso adequados com base nos princípios de privilégio mínimo e. need-to-know	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0489	Implemente medidas de segurança do sistema de acordo com os procedimentos estabelecidos para garantir confidencialidade, integridade, disponibilidade, autenticação e não repúdio.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0491	Instale e configure hardware, software e equipamentos periféricos para usuários do sistema de acordo com os padrões organizacionais.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0491	Instale e configure hardware, software e equipamentos periféricos para usuários do sistema de acordo com os padrões organizac ionais.	ec2-managedinstanc e-association-comp liance-status-check	Use o AWS Systems Manager Associati ons para ajudar no inventário de plataformas e aplicativ os de software em uma organizaç ão. AWS Systems Manager atribui um estado de configura ção às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacion al, instalações de software, configura ções de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0491	Instale e configure hardware, software e equipamentos periféricos para usuários do sistema de acordo com os padrões organizac ionais.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0503	Monitore fontes de dados externas (por exemplo, sites de fornecedores de defesa cibernética, equipes de resposta a emergências de computadores, foco em segurança) para manter a situação atual das ameaças à defesa cibernéti ca e determinar quais problemas de segurança podem ter um impacto na empresa.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
T0509	Realize uma avaliação de risco de segurança da informação.	annual-risk-assess ment-performed (verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabili dade e o impacto dos riscos e/ou vulnerabi lidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	elasticsearch-node-to-node-encryption-check	Certifique-se de que a node-to-node criptografia para o Amazon Elasticse arch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	opensearch-encrypt ed-at-rest	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os domínios do Amazon Elasticsearch Service (Amazon ES).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	opensearch-node-to-node-encryption-check	Certifique-se de que a node-to-node criptografia para o Amazon Elasticsearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	elasticsearch-encrypted-at-rest	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os domínios do Amazon Elasticsearch Service (Amazon ES).
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunid ades de exploração.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0553	Aplique funções de cibersegurança (por exemplo, criptografia, controle de acesso e gerenciamento de identidade) para reduzir as oportunidades de exploração.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
T0557	Integre funções de gerenciamento de chaves relacionadas ao espaço cibernético.	cmk-backing-key-rotation-enabled	Habilite a alternância de chaves para que sejam usadas alternadamente quando atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0557	Integre funções de gerenciamento de chaves relacionadas ao espaço cibernéti co.	kms-cmk-not-schedu led-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessári as não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programad as para exclusão, caso alguma delas sido programada de maneira não intencion al.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0576	Avalie a inteligência de todas as origens e recomende destinos para dar suporte aos objetivos da operação cibernética.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativos da web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticsearch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicação segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositivo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitaç ão do acesso de computadores sem fio e redes digitais.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon Elasticsearch Service (Amazon ES) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Colocar um domínio do Amazon ES no Amazon VPC permite uma comunicação segura entre o Amazon ES e os outros serviços no Amazon VPC, sem que seja necessário usar um gateway da Internet, um dispositivo NAT ou uma conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0609	Conduza a habilitação do acesso de computadores sem fio e redes digitais.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0616	Realize análises de monitoramento e vulnerabilidade de sistemas em uma rede.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0686	Identifique as vulnerabilidades das ameaças.	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0686	Identifique as vulnerabilidades das ameaças.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	elasticsearch-logs-to-cloudwatch	Garanta que os domínios do serviço Amazon Elasticse arch tenham registros de erros habilitad os e transmitidos para o CloudWatch Amazon Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditoria s de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	beanstalk-enhanced -health-reporting- enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	cloudwatch-alarm-a ction-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAc tion Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicionais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0706	Reúna informações sobre redes por meio de técnicas tradicion ais e alternativas (por exemplo, análise de redes sociais, encadeamento de chamadas, análise de tráfego).	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0777	Crie um perfil dos administradores da rede ou do sistema e suas atividades.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0805	Relate eventos e intrusões de rede significativos derivados da inteligência.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0877	Trabalhe em conjunto com as unidades organizacionais aplicáveis na supervisão dos direitos de acesso às informações do consumidor.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0935	Realize uma avaliação de risco de segurança da informação.	annual-risk-assessment-performed (verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultaneidade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitações que a função atende em determinado momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
T0960	Monitore as mudanças em um sistema e em seu ambiente de operação.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-policy-no-stat ements-with-full-a ccess	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizad os, garantindo que as chaves de acesso do IAM sejam alternada s conforme especific ado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorpora r as permissões e autorizações de acesso com os princípios de privilégi o mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autentica r são conhecido s como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principai s se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Managemen t (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Managemen t Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorização contínua.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorização contínua.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	iam-user-unused-cr edentials-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégi o mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	root-account-hardw are-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
T0992	Determine como os resultados do monitoramento contínuo serão usados na autorizaç ão contínua.	secretsmanager-rot ation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
T0993	Estabeleça ferrament as e procedime ntos de controle de acesso a tecnologi as e ferramentas de monitoramento contínuo.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
T0993	Estabeleça ferramentas e procedimentos de controle de acesso a tecnologias e ferramentas de monitoramento contínuo.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 800 181.

Práticas recomendadas operacionais do NIST 1800 25

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST 1800-25 e as regras gerenciadas AWS do Config. Cada um AWS Config se aplica a um AWS recurso específico e está relacionado a um ou mais controles do NIST 1800-25. Um controle NIST 1800-25 pode estar relacionado a várias regras. AWS Config Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
PR.AC-3	O acesso remoto é gerenciado.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.AC-3	O acesso remoto é gerenciado.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-3	O acesso remoto é gerenciado.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-3	O acesso remoto é gerenciado.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.AC-3	O acesso remoto é gerenciado.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-3	O acesso remoto é gerenciado.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-3	O acesso remoto é gerenciado.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-3	O acesso remoto é gerenciado.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciad as, incorporando os princípios de privilégi o mínimo e separação de deveres	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciad as, incorporando os princípios de privilégi o mínimo e separação de deveres	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
PR.DS-1	D ata-at-rest está protegido	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest está protegido	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
PR.DS-1	D ata-at-rest está protegido	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
PR.DS-1	D ata-at-rest está protegido	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
PR.DS-2	D ata-in-transit está protegido	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
PR.DS-2	D ata-in-transit está protegido	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
PR.DS-2	D ata-in-transit está protegido	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
PR.DS-2	D ata-in-transit está protegido	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-6	Mecanismos de verificação de integridade são usados para verificar a integridade de software, firmware e informações	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-6	Mecanismos de verificação de integridade são usados para verificar a integridade de software, firmware e informações	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologi a da informação/ sistemas de controle industrial é criada e mantida incorpora ndo princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-3	Os processos de controle de alterações de configuração estão em vigor	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
PR.IP-3	Os processos de controle de alterações de configuração estão em vigor	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-9	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) estão em vigor e são gerenciados.	response-plan-exists-maintained (Verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável. Ter planos de resposta formalmente atualizados e documentados pode ajudar a garantir que a equipe de resposta compreenda as funções, responsabilidades e processos a serem seguidos durante um incidente.
PR.IP-10	Os planos de resposta e recuperação são testados.	response-plan-tested (Verificação do processo)	Teste os planos de recuperação e resposta a incidentes. Isso pode ajudar a saber se o plano será eficaz durante um incidente e se alguma lacuna ou atualização precisa ser resolvida.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.	vuln-management-plan-exists (Verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente. Isso pode incluir ferramentas de gerenciamento de vulnerabilidades, frequência de análise ambiental, funções e responsabilidades.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.MA-2	A manutenção remota dos ativos organizacionais é aprovada, registrada em log e executada para impedir o acesso não autorizado	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.MA-2	A manutenção remota dos ativos organizac ionais é aprovada, registrada em log e executada para impedir o acesso não autorizado	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	As redes de comunicação e controle são protegidas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.PT-4	As redes de comunicação e controle são protegidas	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-4	As redes de comunicação e controle são protegidas	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem controlada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.PT-4	As redes de comunicação e controle são protegidas	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-4	As redes de comunicação e controle são protegidas	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-4	As redes de comunicação e controle são protegidas	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-4	As redes de comunicação e controle são protegidas	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-4	As redes de comunicação e controle são protegidas	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-8	As varreduras de vulnerabilidade são realizadas.	vuln-scans-perform ed (Verificação do processo)	Garanta que as verificações de vulnerabilidade sejam realizadas de acordo com seus requisito s de conformid ade. A frequência da verificação, as ferramentas usadas e o uso dos resultados devem ser definidos pela sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.MI-3	As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos.	vuln-mitigated-accepted (Verificação do processo)	Garanta que as vulnerabilidades recém-identificadas sejam corrigidas ou documentadas como riscos aceitos. Serviços como o AWS Security Hub, o Amazon Guard Duty, o Amazon Inspector e o AWS Config podem ajudar na identificação de vulnerabilidades em seu ambiente. As vulnerabilidades devem ser corrigidas ou aceitas como riscos de acordo com os requisitos de conformidade da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.MI-3	As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST 1800 25.

Práticas recomendadas operacionais do NIST CSF

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST Cyber Security Framework (CSF) e as regras gerenciadas AWS do Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles do NIST CSF. Um controle da CSF do NIST pode estar relacionado a várias regras de Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	usuários e sistemas é estabelecida e gerenciada		chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os eventos detectados são analisados para entender os alvos e métodos de ataque	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os eventos detectados são analisados para entender os alvos e métodos de ataque	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-1	Os dados do evento são coletados e correlacionados a partir de diversas fontes e sensores	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
DE.AE-4	O impacto dos eventos é determinado	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.AE-4	O impacto dos eventos é determina do	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificações acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-1	A rede é monitorada para detectar possíveis eventos de segurança cibernética	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
DE.CM-3	A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-3	A atividade do pessoal é monitorad a para detectar possíveis eventos de segurança cibernética	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-3	A atividade do pessoal é monitorad a para detectar possíveis eventos de segurança cibernética	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-3	A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-3	A atividade do pessoal é monitorada para detectar possíveis eventos de segurança cibernética	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-3	A atividade do pessoal é monitorad a para detectar possíveis eventos de segurança cibernética	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-4	Um código malicioso é detectado	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-4	Um código malicioso é detectado	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-5	Código móvel não autorizado é detectado	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.
DE.CM-5	Código móvel não autorizado é detectado	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-5	Código móvel não autorizado é detectado	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-5	Código móvel não autorizado é detectado	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-5	Código móvel não autorizado é detectado	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-5	Código móvel não autorizado é detectado	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-6	A atividade do provedor de serviços externo é monitorad a para detecção de possíveis eventos de segurança cibernética	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.CM-7	O monitoramento de pessoal, conexões, dispositivos e software não autorizados é realizado	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.
DE.DP-4	As informações de detecção de eventos são comunicadas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	s3-event-notifications-enabled	As notificações de eventos do Amazon S3 podem alertar equipes relevantes sobre quaisquer modificações acidentais ou intencionais nos objetos do bucket. Os exemplos de alertas incluem: criação de objeto, remoção de objeto, restauração de objeto, objetos perdidos e replicados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-4	As informações de detecção de eventos são comunicadas	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
DE.DP-5	Os processos de detecção são aprimorados continuamente	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instância s do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	Plataformas de software e aplicações dentro da organização são inventariados	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.AM-2	A comunicação organizacional e os fluxos de dados são mapeados	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.BE-5	Os requisitos de resiliência para apoiar a prestação de serviços essenciais são estabelecidos para todos os estados operacionais (por exemplo, sob coação/ataque, durante a recuperação, operações normais)	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-1	As vulnerabilidades de ativos são identificadas e documentadas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-2	A inteligência sobre ameaças cibernéticas é recebida de fóruns e fontes de compartil hamento de informaçõ es	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-3	As ameaças, internas e externas, são identificadas e documentadas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-3	As ameaças, internas e externas, são identificadas e documentadas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
ID.RA-5	Ameaças, vulnerabi lidades, probabili dades e impactos são usados para determinar o risco	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-5	Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-5	Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.RA-5	Ameaças, vulnerabilidades, probabilidades e impactos são usados para determinar o risco	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.SC-4	Fornecedores e parceiros terceiriz ados são avaliados rotineiramente por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar se estão cumprindo suas obrigações contratua is.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
ID.SC-4	Fornecedores e parceiros terceiriz ados são avaliados rotineiramente por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar se estão cumprindo suas obrigações contratua is.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.SC-4	Fornecedores e parceiros terceirizados são avaliados rotineiramente por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar se estão cumprindo suas obrigações contratuais.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.SC-4	Fornecedores e parceiros terceiriz ados são avaliados rotineiramente por meio de auditorias, resultados de testes ou outras formas de avaliação para confirmar se estão cumprindo suas obrigações contratua is.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Algun s desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-1	As identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.AC-3	O acesso remoto é gerenciado.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-3	O acesso remoto é gerenciado.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-3	O acesso remoto é gerenciado.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.AC-3	O acesso remoto é gerenciado.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-3	O acesso remoto é gerenciado.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-3	O acesso remoto é gerenciado.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-3	O acesso remoto é gerenciado.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-3	O acesso remoto é gerenciado.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-3	O acesso remoto é gerenciado.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciad as, incorporando os princípios de privilégi o mínimo e separação de deveres	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciad as, incorporando os princípios de privilégi o mínimo e separação de deveres	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciad as, incorporando os princípios de privilégi o mínimo e separação de deveres	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-6	As identidades são comprovadas e vinculadas às credenciais e declaradas nas interações	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-6	As identidades são comprovadas e vinculadas às credenciais e declaradas nas interações	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	iam-user-mfa-enabled	Habilite essa regra para restringir o acesso a recursos na Nuvem AWS . Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-7	Usuários, dispositivos e outros ativos são autenticados (por exemplo, fator único, multifator) de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais)	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AT-1	Todos os usuários são informados e treinados	security-awareness -program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organizaç ão. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
PR.DS-1	D ata-at-rest está protegido	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
PR.DS-1	D ata-at-rest está protegido	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
PR.DS-1	D ata-at-rest está protegido	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
PR.DS-1	D ata-at-rest está protegido	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
PR.DS-1	D ata-at-rest está protegido	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-1	D ata-at-rest está protegido	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-1	D ata-at-rest está protegido	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
PR.DS-2	D ata-in-transit está protegido	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
PR.DS-2	D ata-in-transit está protegido	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
PR.DS-2	D ata-in-transit está protegido	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-2	D ata-in-transit está protegido	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
PR.DS-2	D ata-in-transit está protegido	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-3	Os ativos são gerenciados formalmente durante a remoção, transferência e descarte	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-3	Os ativos são gerenciados formalmente durante a remoção, transferência e descarte	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-3	Os ativos são gerenciados formalmente durante a remoção, transferência e descarte	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-4	Capacidade adequada para garantir que a disponibilidade seja mantida	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	codebuild-project-envvar-awscred-check	Certifique-se de que as credencia is de autentica ção AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptogra fado. Armazenar essas variáveis em texto não criptogra fado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.DS-5	Proteções contra vazamentos de dados são implementadas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-6	Mecanismos de verificação de integridade são usados para verificar a integridade de software, firmware e informações	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-6	Mecanismos de verificação de integridade são usados para verificar a integridade de software, firmware e informações	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-7	Os ambientes de desenvolvimento e teste são separados do ambiente de produção	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologi a da informação/ sistemas de controle industrial é criada e mantida incorpora ndo princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interromp idas por mais dias do que o permitido pelos padrões da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-1	Uma configuração básica de tecnologia da informação/ sistemas de controle industrial é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade)	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-2	Um ciclo de vida de desenvolvimento do sistema para gerenciar sistemas é implementado	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-2	Um ciclo de vida de desenvolvimento do sistema para gerenciar sistemas é implementado	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-2	Um ciclo de vida de desenvolvimento do sistema para gerenciar sistemas é implementado	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-3	Os processos de controle de alterações de configuração estão em vigor	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
PR.IP-3	Os processos de controle de alterações de configuração estão em vigor	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-4	Os backups das informações são conduzidos, mantidos e testados	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-7	Os processos de proteção são aprimorados	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.
PR.IP-8	A eficácia das tecnologias de proteção é compartilhada	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	ec2-instance-no-pu blic-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartilhada	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.IP-8	A eficácia das tecnologias de proteção é compartil hada	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS Systems Manager atribui um estado de configuração às instâncias gerenciadas e permite que você defina linhas de base de níveis de patch do sistema operacional, instalações de software, configurações de aplicações e outros detalhes sobre o ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.IP-12	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.MA-2	A manutenção remota dos ativos organizacionais é aprovada, registrada em log e executada para impedir o acesso não autorizado	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.MA-2	A manutenção remota dos ativos organizac ionais é aprovada, registrada em log e executada para impedir o acesso não autorizado	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	As redes de comunicação e controle são protegidas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem informações da conta da AWS que acessou um bucket do Amazon S3, o endereço IP e o horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-1	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	lambda-function-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-3	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.PT-4	As redes de comunicação e controle são protegidas	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-4	As redes de comunicação e controle são protegidas	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.PT-4	As redes de comunicação e controle são protegidas	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-4	As redes de comunicação e controle são protegidas	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-4	As redes de comunicação e controle são protegidas	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-4	As redes de comunicação e controle são protegidas	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-4	As redes de comunicação e controle são protegidas	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegidas	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-4	As redes de comunicação e controle são protegida s	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	dynamodb-autoscali ng-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidad e de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidad e provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-5	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RC.RP-1	O plano de recuperação é executado durante ou após um incidente de cibersegurança	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.AN-2	O impacto do incidente é compreendido	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.MI-3	As vulnerabilidades recém-identificadas são mitigadas ou documentadas como riscos aceitos	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDaysConfig default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
RS.RP-1	O plano de resposta é executado durante ou após um incidente	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
RS.RP-1	O plano de resposta é executado durante ou após um incidente	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
RS.RP-1	O plano de resposta é executado durante ou após um incidente	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
RS.RP-1	O plano de resposta é executado durante ou após um incidente	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST CSF.

Práticas recomendadas operacionais para o NIST Privacy Framework v1.0

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o NIST Privacy Framework e as regras gerenciadas do AWS Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles do NIST Privacy Framework. Um controle do NIST Privacy Framework pode estar relacionado a várias AWS Config regras. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissões de processamento e valores de dados relacionados a elementos de dados.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissõe	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	s de processam ento e valores de dados relacionados a elementos de dados.		para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissõe s de processam ento e valores de dados relacionados a elementos de dados.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissões de processamento e valores de dados relacionados a elementos de dados.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissõe s de processam ento e valores de dados relacionados a elementos de dados.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissõe s de processam ento e valores de dados relacionados a elementos de dados.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissões de processamento e valores de dados relacionados a elementos de dados.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissões de processamento e valores de dados relacionados a elementos de dados.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P7	Há mecanismos estabelecidos e implementados para transmitir permissões de processamento e valores de dados relacionados a elementos de dados.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	audit-log-policy-exists (verificação de processo)	Estabeleça e mantenha uma política de gerenciamento de logs de auditoria que defina os requisitos de registro em log de sua organização. Isso inclui, entre outras coisas, a revisão e retenção de logs de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapass a o limite de um número específico de períodos de avaliação . O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimizaç ão de dados.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
CT.DM-P8	Os registros de auditoria/log são determinados, documentados, implementados e revisados de acordo com a política e integração do princípio de minimização de dados.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
ID.DE-P2	As partes do ecossistema de processamento de dados (por exemplo, provedores de serviços, clientes, parceiros, fabricantes de produtos, desenvolvedores de aplicativos) são identificadas, priorizadas e avaliadas usando um processo de avaliação de risco de privacidade.	annual-risk-assessment-performed (verificação de processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
PR.AC-P1	Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-P3	O acesso remoto é gerenciado.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-P3	O acesso remoto é gerenciado.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
PR.AC-P3	O acesso remoto é gerenciado.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-P3	O acesso remoto é gerenciado.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4433). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-P3	O acesso remoto é gerenciado.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-P3	O acesso remoto é gerenciado.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P3	O acesso remoto é gerenciado.	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-P4	As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de deveres.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P5	A integridade da rede é protegida (por exemplo, segregação de rede, segmentação de rede).	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P6	Indivíduos e dispositivos são comprovados e vinculados a credenciais e autenticados de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P6	Indivíduos e dispositivos são comprovados e vinculados a credenciais e autenticados de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P6	Indivíduos e dispositivos são comprovados e vinculados a credenciais e autenticados de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P6	Indivíduos e dispositivos são comprovados e vinculados a credenciais e autenticados de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.AC-P6	Indivíduos e dispositivos são comprovados e vinculados a credenciais e autenticados de acordo com o risco da transação (por exemplo, riscos de segurança e privacidade de indivíduos e outros riscos organizacionais).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
PR.DS-P1	D ata-at-rest estão protegidos.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
PR.DS-P1	D ata-at-rest estão protegidos.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-P1	D ata-at-rest estão protegidos.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
PR.DS-P1	D ata-at-rest estão protegidos.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, garanta que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-P1	D ata-at-rest estão protegidos.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-P1	D ata-at-rest estão protegidos.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptogra fia em repouso para ajudar a protegê-los.
PR.DS-P1	D ata-at-rest estão protegidos.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P1	D ata-at-rest estão protegidos.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
PR.DS-P2	D ata-in-transit estão protegidos.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P2	D ata-in-transit estão protegidos.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.
PR.DS-P2	D ata-in-transit estão protegidos.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P2	D ata-in-transit estão protegidos.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
PR.DS-P2	D ata-in-transit estão protegidos.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P4	Capacidade adequada para garantir que a disponibilidade seja mantida.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	codebuild-project-envvar-awscred-check	Certifique-se de que as credencia is de autentica ção AWS_ACCES S_KEY_ID e AWS_SECRE T_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptogra fado. Armazenar essas variáveis em texto não criptogra fado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P5	Proteções contra vazamentos de dados são implementadas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.DS-P6	Mecanismos de verificação de integridade são usados para verificar a integridade de software, firmware e informações.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.
PR.MA-P2	A manutenção remota dos ativos organizac ionais é aprovada, registrada em log e executada para impedir o acesso não autorizado.	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.MA-P2	A manutenção remota dos ativos organizac ionais é aprovada, registrada em log e executada para impedir o acesso não autorizado.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologi a da informação é criada e mantida incorporando princípio s de segurança (por exemplo, conceito de menor funcional idade).	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomendadas para AWS CloudTrail, verificando a ativação de várias configura ções. Isso inclui o uso de criptogra fia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar com o inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologi a da informação é criada e mantida incorporando princípio s de segurança (por exemplo, conceito de menor funcional idade).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Uma configuração básica da tecnologia da informação é criada e mantida incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
AT-1: PR.PO-P10	Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.	vuln-management-plan-exists (verificação de processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P1	Processos de controle de alterações de configuração foram estabelecidos e estão em vigor.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
PR.PO-P1	Processos de controle de alterações de configuração foram estabelecidos e estão em vigor.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P3	Os backups das informações são conduzidos, mantidos e testados.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidente s e continuidade de negócios) e planos de recuperaç ão (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PO-P7	Planos de resposta (resposta a incidentes e continuidade de negócios) e planos de recuperação (recuperação de incidentes e recuperação de desastres) foram estabelecidos, implementados e gerenciados.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
PR.PO-P8	Os planos de resposta e recuperação são testados.	response-plan-tested (verificação de processo)	Teste os planos de recuperação e resposta a incidentes. Isso pode ajudar a saber se o plano será eficaz durante um incidente e se alguma lacuna ou atualização precisa ser resolvida.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.PT-P2	O princípio de funcionalidade mínima é incorporado pela configuração de sistemas para fornecer somente recursos essenciais	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P2	O princípio de funcionalidade mínima é incorpora do pela configura ção de sistemas para fornecer somente recursos essenciais	redshift-enhanced-vpc-routing-enabled	O roteamento aprimorado da VPC força todo o tráfego de COPY e UNLOAD entre o cluster e os repositórios de dados a passar pelo Amazon VPC. Em seguida, você pode usar recursos da VPC, como grupos de segurança e listas de controle de acesso à rede, para proteger o tráfego da rede. Você também pode usar os logs de fluxo da VPC para monitorar o tráfego da rede.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegida s.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-P3	As redes de comunicação e controle são protegidas.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
PR.PT-P3	As redes de comunicação e controle são protegidas.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
PR.PT-P3	As redes de comunicação e controle são protegidas.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
PR.PT-P3	As redes de comunicação e controle são protegidas.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
PR.PT-P3	As redes de comunicação e controle são protegidas.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
PR.PT-P3	As redes de comunicação e controle são protegidas.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
PR.PT-P3	As redes de comunicação e controle são protegidas.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegida s.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.
PR.PT-P3	As redes de comunicação e controle são protegidas.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
PR.PT-P3	As redes de comunicação e controle são protegidas.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P3	As redes de comunicação e controle são protegidas.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	dynamodb-autoscali ng-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidad e de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidad e provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	dynamodb-pitr-enab led	Habilite essa regra para verificar se o backup das informaçõ es foi realizado. Ele também mantém os backups, garantind o que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	elb-deletion-prote ction-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitad a. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	aurora-resources-p rotected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	backup-plan-min-fr equency-and-min-re tention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyV alue parâmetros (Config default: 1), (requiredRetentionD ays Config default: 35) e (requiredF requencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperaç ão. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionD ays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	ec2-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
PR.PT-P4	Mecanismos (por exemplo, proteção contra falhas, balanceamento de carga, troca a quente) são implement ados para atingir os requisitos de resiliênc ia em situações normais e adversas.	fsx-resources-prot ected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NIST Privacy Framework v1.0.

Práticas recomendadas operacionais para o NYDFS 23

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é

responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre os requisitos de segurança cibernética do Departamento de Serviços Financeiros do Estado de Nova York (NYDFS) para empresas de serviços financeiros (23 NYCRR 500) e as regras gerenciadas do Config. AWS Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles do NYDFS dos EUA. Um controle do US NYDFS 23 NYCRR 500 pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.		o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	api-gw-cache-enabl ed-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturado s para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	kinesis-stream-enc rypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Kinesis Streams.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenc iais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elb-cross-zone-load-balancing-enabled	Habilite o balanceam ento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidad e e a disponibi lidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibi lidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instância s do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibi lidade das aplicações.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	autoscaling-launch -config-public-ip- disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	backup-recovery-po int-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	beanstalk-enhanced -health-reporting- enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identific ados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	dynamodb-table-enc rypted-kms	Habilite a criptogra fia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernética concebido para proteger a confidencialidade, integridade e disponibilidade dos Sistemas de Informação da Entidade Coberta.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	opensearch-node-to -node-encryption-c heck	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(a)	(a) Programa de cibersegurança. Cada Entidade Coberta deverá manter um programa de segurança cibernéti ca concebido para proteger a confidenc ialidade, integrida de e disponibilidade dos Sistemas de Informação da Entidade Coberta.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	root-account-mfa-e nabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitad a para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	sagemaker-notebook -no-direct-internet- access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-inten cionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernéti ca deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de segurança cibernéti ca: (2) use infraestr utura defensiva e a implementação de políticas e procedime ntos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenad as nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(2)	(b) O programa de segurança cibernética deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de segurança cibernética: (2) use infraestrutura defensiva e a implementação de políticas e procedimentos para proteger os Sistemas de Informação da Entidade Coberta e as Informações Não Públicas armazenadas nesses Sistemas de Informação contra acesso, uso ou outros atos maliciosos não autorizados.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositi vos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	api-gw-execution-l ogging-enabled	O registro em log do API Gateway exibe visualiza ções detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralme nte a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearc h Service tenham registros de erros habilitados e transmiti dos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosti car problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenhar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatc h ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informaçõ es detalhadas sobre o projeto de compilaçã o.
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(3)	(b) O programa de cibersegurança deve ser baseado na Avaliação de Risco da Entidade Coberta e projetado para desempenh ar as seguintes funções principais de cibersegurança: (3) detecte eventos de cibersegurança.	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	redshift-backup-en abled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernética será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernética: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
500.02(b)(5)	(b) O programa de segurança cibernética será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernética: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernéti ca será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernéti ca: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relationa l Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.02(b)(5)	(b) O programa de segurança cibernética será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernética: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
500.02(b)(5)	(b) O programa de segurança cibernética será baseado na Avaliação de Risco da Entidade Coberta e projetado para executar as seguintes funções principais de segurança cibernética: (5) recupere-se de Eventos de Segurança Cibernética e restaure operações e serviços normais.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,05	O programa de segurança cibernéti ca para cada entidade coberta deve incluir monitoramento e testes, desenvolv idos de acordo com a avaliação de risco da entidade coberta, projetados para avaliar a eficácia do programa de segurança cibernética da entidade coberta. O monitoramento e os testes devem incluir monitoram ento contínuo ou testes de penetraçã o e avaliações de vulnerabilidade periódicos. Na ausência de um monitoramento contínuo eficaz ou de outros sistemas para detectar, de forma contínua, mudanças nos sistemas de informação que possam criar ou indicar vulnerabi lidades, as entidades	vuln-management-pl an-exists (verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	cobertas devem realizar: (a) testes anuais de penetraçã o dos sistemas de informação da entidade coberta determinados a cada ano com base nos riscos relevante s identificados de acordo com a avaliação de risco; e (b) avaliações de vulnerabilidade semestrais, incluindo quaisquer verificações ou revisões sistemáti cas dos sistemas de informação razoavelm ente concebidas para identificar vulnerabi lidades de segurança cibernética publicame nte conhecidas nos sistemas de informação da entidade coberta com base na avaliação de riscos.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transaçõe s financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetada s para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabili dade razoável de prejudicar materialm ente qualquer parte material das operações normais da Entidade Coberta.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transaçõe s financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetada s para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabili dade razoável de prejudicar materialm ente qualquer parte material das operações normais da Entidade Coberta.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transaçõe s financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetada s para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabili dade razoável de prejudicar materialm ente qualquer parte material das operações normais da Entidade Coberta.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transaçõe s financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetada s para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabili dade razoável de prejudicar materialm ente qualquer parte material das operações normais da Entidade Coberta.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transaçõe s financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetada s para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabili dade razoável de prejudicar materialm ente qualquer parte material das operações normais da Entidade Coberta.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(b)	(b) Cada Entidade Coberta deverá manter os registros exigidos pela seção 500.06(a)(1) desta Parte por pelo menos cinco anos e deverá manter os registros exigidos pela seção 500.06(a)(2) desta Parte por pelo menos três anos.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.06(a)	(a) Cada Entidade Coberta deverá manter de forma segura sistemas que, na medida do aplicável e com base na sua Avaliação de Risco: (1) sejam concebidos para reconstruir transações financeiras materiais suficientes para apoiar as operações e obrigações normais da Entidade Coberta; e (2) incluam trilhas de auditoria projetadas para detectar e responder a Eventos de Segurança Cibernética que tenham uma probabilidade razoável de prejudicar materialmente qualquer parte material das operações normais da Entidade Coberta.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	ecs-task-definition-user-for-host-mode-check	Se uma definição de tarefa tem privilégios elevados, significa que o cliente optou especificamente por essas configurações. Esse controle verifica o aumento inesperado de privilégios quando uma definição de tarefa tem a rede de host habilitada e o cliente não optou por privilégios elevados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciad as e verificadas com base em uma política organizac ional de senhas do IAM. Eles atendem ou excedem os requisitos estabelec idos pelo NIST SP 800-63 e pelo padrão AWS Foundatio nal Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCh aracters (valor das melhores práticas de segurança AWS básicas: verdadeir o), RequireSy mbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernéti ca, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,07	Como parte do seu programa de segurança cibernética, com base na Avaliação de Risco da Entidade Coberta, cada Entidade Coberta limitará os privilégios de acesso do usuário aos Sistemas de Informação que fornecem acesso a Informações Não Públicas e revisará periodicamente esses privilégios de acesso.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.8(a)	(a) O programa de segurança cibernética de cada entidade coberta deverá incluir procedimentos escritos, diretrizes e padrões projetados para garantir o uso de práticas de desenvolvimento seguras para aplicações desenvolvidas internamente e utilizadas pela entidade coberta e procedimentos para avaliar ou testar a segurança de aplicações desenvolvidas externamente utilizadas pela entidade coberta no contexto do ambiente tecnológico da entidade coberta.	codebuild-project-envvar-awscred-check	Certifique-se de que as credenciais de autenticação AWS_ACCESS_KEY_ID e AWS_SECRET_ACCESS_KEY não existam nos ambientes do projeto Codebuild. AWS Não armazene essas variáveis em texto não criptografado. Armazenar essas variáveis em texto não criptografado pode causar exposição não intencional dos dados e acesso não autorizado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.8(a)	(a) O programa de segurança cibernética de cada entidade coberta deverá incluir procedimentos escritos, diretrizes e padrões projetados para garantir o uso de práticas de desenvolvimento seguras para aplicações desenvolvidas internamente e utilizadas pela entidade coberta e procedimentos para avaliar ou testar a segurança de aplicações desenvolvidas externamente utilizadas pela entidade coberta no contexto do ambiente tecnológico da entidade coberta.	codebuild-project-source-repo-url-check	Certifique-se de que o GitHub URL do repositório de origem do Bitbucket não contenha tokens de acesso pessoais e credenciais de login nos ambientes do projeto Codebuild . AWS Use OAuth em vez de tokens de acesso pessoal ou credenciais de login para conceder autorização para acessar nossos repositórios do Bitbucket. GitHub

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,09	(a) Cada entidade coberta deve realizar uma avaliação periódica de risco dos sistemas de informação da entidade coberta, suficiente para informar a concepção do programa de segurança cibernéti ca, conforme exigido por esta Parte. Essa avaliação de risco deve ser atualizada conforme razoavelm ente necessário para lidar com alteraçõe s nos sistemas de informação, informaçõ es não públicas ou operações comerciai s da entidade coberta. A avaliação de risco da entidade coberta deverá permitir a revisão dos controles para responder aos desenvolvimentos tecnológicos e às ameaças em evolução e deverá considerar os riscos	annual-risk-assess ment-performed (verificação do processo) >	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabili dade e o impacto dos riscos e/ou vulnerabi lidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	específicos das operações comerciais da entidade coberta relacionadas à segurança cibernética, informações não públicas coletadas ou armazenadas, sistemas de informação utilizados e a disponibilidade e eficácia de controles para proteger informações não públicas e sistemas de informação.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,12	(a) Autenticação multifator. Com base na sua Avaliação de Risco, cada Entidade Coberta deverá utilizar controles eficazes, que podem incluir Autentica ção Multifatorial ou Autenticação Baseada em Risco, para proteger contra acesso não autorizad o a Informações Não Públicas ou Sistemas de Informação. (b) A autenticação multifator deverá ser utilizada para qualquer indivíduo que acesse as redes internas da Entidade Coberta a partir de uma rede externa, a menos que o CISO da Entidade Coberta tenha aprovado por escrito o uso de controles de acesso razoavelm ente equivalentes ou mais seguros.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,12	(a) Autenticação multifator. Com base na sua Avaliação de Risco, cada Entidade Coberta deverá utilizar controles eficazes, que podem incluir Autentica ção Multifatorial ou Autenticação Baseada em Risco, para proteger contra acesso não autorizad o a Informações Não Públicas ou Sistemas de Informação. (b) A autenticação multifator deverá ser utilizada para qualquer indivíduo que acesse as redes internas da Entidade Coberta a partir de uma rede externa, a menos que o CISO da Entidade Coberta tenha aprovado por escrito o uso de controles de acesso razoavelm ente equivalentes ou mais seguros.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,12	(a) Autenticação multifator. Com base na sua Avaliação de Risco, cada Entidade Coberta deverá utilizar controles eficazes, que podem incluir Autentica ção Multifatorial ou Autenticação Baseada em Risco, para proteger contra acesso não autorizad o a Informações Não Públicas ou Sistemas de Informação. (b) A autenticação multifator deverá ser utilizada para qualquer indivíduo que acesse as redes internas da Entidade Coberta a partir de uma rede externa, a menos que o CISO da Entidade Coberta tenha aprovado por escrito o uso de controles de acesso razoavelm ente equivalentes ou mais seguros.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,12	(a) Autenticação multifator. Com base na sua Avaliação de Risco, cada Entidade Coberta deverá utilizar controles eficazes, que podem incluir Autenticação Multifatorial ou Autenticação Baseada em Risco, para proteger contra acesso não autorizado a Informações Não Públicas ou Sistemas de Informação. (b) A autenticação multifator deverá ser utilizada para qualquer indivíduo que acesse as redes internas da Entidade Coberta a partir de uma rede externa, a menos que o CISO da Entidade Coberta tenha aprovado por escrito o uso de controles de acesso razoavelmente equivalentes ou mais seguros.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,12	(a) Autenticação multifator. Com base na sua Avaliação de Risco, cada Entidade Coberta deverá utilizar controles eficazes, que podem incluir Autenticação Multifatorial ou Autenticação Baseada em Risco, para proteger contra acesso não autorizado a Informações Não Públicas ou Sistemas de Informação. (b) A autenticação multifator deverá ser utilizada para qualquer indivíduo que acesse as redes internas da Entidade Coberta a partir de uma rede externa, a menos que o CISO da Entidade Coberta tenha aprovado por escrito o uso de controles de acesso razoavelmente equivalentes ou mais seguros.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	cloudwatch-alarm-action-check	CloudWatch Os alarmes da Amazon alertam quando uma métrica ultrapassa o limite de um número específico de períodos de avaliação. O alarme executa uma ou mais ações com base no valor da métrica ou na expressão em relação a um limite em alguns períodos. Essa regra exige um valor para alarmActionRequired (Config Default: True), insufficientDataAction Obrigatório (Config Default: True), (okActionRequired Config Default: False). O valor real deve refletir as ações de alarme do ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informações como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500.14(a)	(a) implemente políticas, procedimentos e controles baseados em risco projetados para monitorar a atividade de Usuários Autorizados e detecte acesso não autorizado, uso ou adulteração de Informações Não Públicas por tais Usuários Autorizados.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,14 (b)	Como parte de seu programa de segurança cibernética, cada entidade coberta deve: (b) fornecer treinamento regular de conscientização sobre cibersegurança para todo o pessoal, atualizado para refletir os riscos identificados pela entidade coberta em sua avaliação de risco.	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	elasticsearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernéti ca, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles , incluindo criptogra fia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,15 (a)	(a) Como parte de seu programa de segurança cibernética, com base em sua Avaliação de Risco, cada Entidade Coberta deve implementar controles, incluindo criptografia, para proteger as Informações Não Públicas mantidas ou transmitidas pela Entidade Coberta, tanto em trânsito por redes externas quanto em repouso.	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Kinesis Streams.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
500,16	(a) Como parte de seu programa de segurança cibernética, cada entidade coberta deve estabelecer um plano escrito de resposta a incidentes projetado para responder e se recuperar prontamente de qualquer evento de cibersegurança que afete materialmente a confidencialidade, integridade ou disponibilidade dos sistemas de informação da entidade coberta ou a funcionalidade contínua de qualquer aspecto dos negócios ou operações da entidade coberta.	response-plan-exists-maintained (verificação do processo)	Garanta que os planos de resposta a incidentes sejam estabelecidos, mantidos e distribuídos à equipe responsável.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NYDFS 23.

Práticas recomendadas operacionais para o CIS

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config

Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Manual de Segurança da Informação (NZISM) 2022-09, versão 3.6, do Departamento de Segurança das Comunicações do Governo da Nova Zelândia (GCSB), e as regras do Managed Config. AWS Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles NZISM. Um controle do NZISM pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

Este exemplo de modelo de pacote de conformidade contém mapeamentos para controles dentro da estrutura NZISM, que é parte integrante da estrutura de Requisitos de Segurança de Proteção (PSR) que define as expectativas do governo da Nova Zelândia em relação ao gerenciamento de pessoal, informações e segurança física.

O NZISM está licenciado sob a licença do Creative Commons Attribution 4.0 da Nova Zelândia, disponível em https://creativecommons.org/licenses/by/4.0/. Informações sobre direitos autorais podem ser encontradas no Manual de Segurança da Informação NZISM da Nova Zelândia | Legal, Privacidade e Direitos Autorais.

ID de controle	AWS Regra de configuração	Orientação
1149	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome

ID de controle	AWS Regra de configuração	Orientação
		do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
1149	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
1149	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	AWS Regra de configuração	Orientação
1149	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.
1149	ec2- hardening-and-state-management (Verificação do processo)	Os processos reforçados de criação de imagens do servidor EC2 e as associações de gerentes estaduais são configurados para remover componentes e serviços desnecessários e instalar software antimalware e agentes de log.

ID de controle	AWS Regra de configuração	Orientação
161	cloudfront-default-root-object-configured	Esse controle verifica se uma CloudFront distribuição da Amazon está configura da para retornar um objeto específico que é o objeto raiz padrão. O controle falhará se a CloudFront distribuição não tiver um objeto raiz padrão configurado. Às vezes, um usuário pode solicitar o URL raiz da distribuição, em vez de um objeto na distribuição. Quando isso acontece, a especificação de um objeto raiz padrão pode ajudá-lo a evitar a exposição do conteúdo de sua distribuição da web. Essa regra deve ser aplicada na região leste dos EUA-1.
167	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
167	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
1841	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	AWS Regra de configuração	Orientação
1841	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
1841	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
1841	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS
1847	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
1847	cloudfront-viewer-policy-https	Esse controle verifica se uma CloudFront distribui ção da Amazon exige que os espectadores usem HTTPS diretamente ou se ela usa redirecionamento. O controle falhará se ViewerPro tocolPolicy estiver configura do para permitir tudo para defaultCacheBehavior ou para CacheBehaviors. O HTTPS (TLS) pode ser usado para ajudar a impedir que possíveis invasores usem ataques semelhantes para espionar person-in-the-midd le ou manipular o tráfego da rede. Somente conexões criptografadas por HTTPS (TLS) devem ser permitidas. Essa regra deve ser aplicada na região leste dos EUA-1.

ID de controle	AWS Regra de configuração	Orientação
1847	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
1847	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
1847	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
1858	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
1893	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
1893	federate-with-central-idp (Verificação do processo)	As identidades da força de trabalho que exigem acesso aos AWS recursos são autenticadas com um IdP central que é federado com SSO. AWS O IdP central bloqueia os usuários do sistema após três tentativas malsucedidas de login.

ID de controle	AWS Regra de configuração	Orientação
1946	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
1946	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
1998	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
1998	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
1998	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.

ID de controle	AWS Regra de configuração	Orientação
2013	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
2013	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
2013	cloudfront-accesslogs-enabled	Esse controle verifica se o registro de acesso ao servidor está habilitado nas CloudFron t distribuições. O controle falhará se o registro em log de acesso não estiver habilitad o para uma distribuição. CloudFront os registros de acesso fornecem informaçõ es detalhadas sobre cada solicitação do usuário que CloudFront recebe. Cada registro em log contém informações como a data e a hora em que a solicitação foi recebida, o endereço IP do visualizador que fez a solicitaç ão, a origem da solicitação e o número da porta da solicitaç ão do visualizador. Esses logs são úteis para aplicações como auditorias de segurança e acesso e investigação forense. Essa regra deve ser aplicada na região leste dos EUA-1.

ID de controle	AWS Regra de configuração	Orientação
2013	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
2013	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.

ID de controle	AWS Regra de configuração	Orientação
2013	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
2022	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.
2022	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
2028	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.
2082	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los. Uma isenção está disponível para ambientes de pré-produção.
2082	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.

ID de controle	AWS Regra de configuração	Orientação
2082	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
2082	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
2082	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
2082	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	AWS Regra de configuração	Orientação
2082	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
2082	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
2082	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2082	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
2082	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
2019	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2019	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2019	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2598	elb-custom-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, certifiqu e-se de que seus ouvintes ElasticLoadBalancer SSL clássicos estejam usando uma política de segurança personalizada. Essas políticas podem fornecer vários algoritmos criptográficos de alta resistência para ajudar a garantir comunicações de rede criptografadas entre sistemas. Essa regra exige que você defina uma política de segurança personalizada para seus receptores de SSL. A política de segurança padrão é: Protocol-TLSv1.2, ECDHE-ECDSA-AES128-GCM-SHA256.

ID de controle	AWS Regra de configuração	Orientação
2600	elb-custom-security-policy-ssl-check	Para ajudar a proteger os dados em trânsito, certifiqu e-se de que seus ouvintes ElasticLoadBalancer SSL clássicos estejam usando uma política de segurança personalizada. Essas políticas podem fornecer vários algoritmos criptográficos de alta resistência para ajudar a garantir comunicações de rede criptografadas entre sistemas. Essa regra exige que você defina uma política de segurança personalizada para seus receptores de SSL. A política de segurança padrão é: Protocol-TLSv1.2, ECDHE-ECDSA-AES128-GCM-SHA256.
2726	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
3021	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
3021	kms-cmk- for-each-data-classification (Verificação do processo)	Pelo menos uma chave mestra de cliente (CMK) do KMS foi definida para cada classificação de dados distinta, e as CMKs estão sendo usadas para criptografar todos os dados armazenados nessa classificação.
3205	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
3449	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
3449	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	AWS Regra de configuração	Orientação
3449	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automatedSnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
3451	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
3451	ec2-critical- security-patch-auto-approval (Verificação do processo)	As listas de referência de patches para Windows e/ou Linux foram configuradas no Patch Manager, incluindo a aprovação automática de patches de segurança críticos em até dois dias após o lançamento.
3452	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
3452	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
3452	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.
3453	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
3453	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
3562	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
3562	cloudfront-associated-with-waf	Esse controle verifica se CloudFront as distribuições estão associadas às ACLs da web AWS WAF ou AWS WAFv2. O controle falhará se a distribuição não estiver associada a uma ACL da web. AWS O WAF é um firewall de aplicativos da web que ajuda a proteger aplicativos e APIs da web contra ataques. Permite configurar um conjunto de regras, chamado de lista de controle de acesso à web (ACL da web) que permitem, bloqueiam ou contam solicitaç ões da web com base em regras e condições que você define. Certifique-se de que sua CloudFront distribuição esteja associada a uma Web ACL AWS do WAF para ajudar a protegê-la contra ataques maliciosos. Essa regra deve ser aplicada na região leste dos EUA-1.

ID de controle	AWS Regra de configuração	Orientação
3562	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
3562	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	AWS Regra de configuração	Orientação
3562	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
3562	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
3562	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
3562	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
3562	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.
3562	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
3562	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
3562	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
3562	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
3562	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
3562	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
3562	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
3562	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
3623	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
3623	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
3623	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
3623	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
3815	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
3875	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
3875	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS
4333	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
4441	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
4441	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
4441	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.

ID de controle	AWS Regra de configuração	Orientação
4441	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
4441	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
4441	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4441	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
4445	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.

ID de controle	AWS Regra de configuração	Orientação
4445	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
4829	dynamodb-autoscaling-enable d	O Amazon DynamoDB auto scaling usa o serviço Applicati on AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automatic amente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentino s no tráfego, sem controle de utilização.

ID de controle	AWS Regra de configuração	Orientação
4829	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	AWS Regra de configuração	Orientação
4829	rds-cluster-multi-az-enabled	Os clusters do Amazon Relational Database Service (Amazon RDS) devem ter a replicação multi-AZ habilitad a para auxiliar na disponibi lidade dos dados armazenad os. Cada zona de disponibi lidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
4829	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instância s de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automatic amente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	AWS Regra de configuração	Orientação
4838	cloudtrail-s3-dataevents-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.
4838	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
4838	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
4838	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
4838	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
4839	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenciais em repouso nessas tabelas, habilite a criptografia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.
4839	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para o Amazon Elastic File System (EFS).

ID de controle	AWS Regra de configuração	Orientação
4839	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .
4839	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
4839	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4839	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
4839	opensearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitad a para seus domínios do Amazon OpenSearch Service.
4839	opensearch-node-to-node-enc ryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4839	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptogra fia em repouso para ajudar a protegê-los.
4839	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4839	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
4839	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4839	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
4839	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
4839	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.
4839	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4839	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
4849	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.

ID de controle	AWS Regra de configuração	Orientação
4849	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
4849	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	AWS Regra de configuração	Orientação
4849	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
4849	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
4849	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
4849	rds-cluster-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
4849	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
4849	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	AWS Regra de configuração	Orientação
4849	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.
4849	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
6843	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
6843	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
6852	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especific ado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.
6852	federate-with-central-idp (Verificação do processo)	As identidades da força de trabalho que exigem acesso aos AWS recursos são autenticadas com um IdP central que é federado com SSO. AWS O IdP central bloqueia os usuários do sistema após três tentativas malsucedidas de login.

ID de controle	AWS Regra de configuração	Orientação
6860	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
6860	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
6861	cloudtrail-security-trail-enabled	Essa regra ajuda a garantir o uso das melhores práticas de segurança AWS recomenda das para AWS CloudTrai l, verificando a ativação de várias configurações. Isso inclui o uso de criptografia de registros, validação de registros e habilitação AWS CloudTrail em várias regiões.

ID de controle	AWS Regra de configuração	Orientação
6953	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Managemen t (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credencia is de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.
6953	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
7436	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
7436	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
7436	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
7436	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
7437	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
7437	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
7437	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
7437	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
7466	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.
7466	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
7466	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.
7466	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
7466	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
7466	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
7466	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
7466	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.
7466	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
7466	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.
7466	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
7466	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
7466	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
7466	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
7466	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.
7466	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	AWS Regra de configuração	Orientação
7466	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
7496	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
7496	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
7496	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
7496	cloudfront-accesslogs-enabled	Esse controle verifica se o registro de acesso ao servidor está habilitado nas CloudFron t distribuições. O controle falhará se o registro em log de acesso não estiver habilitad o para uma distribuição. CloudFront os registros de acesso fornecem informaçõ es detalhadas sobre cada solicitação do usuário que CloudFront recebe. Cada registro em log contém informações como a data e a hora em que a solicitação foi recebida, o endereço IP do visualizador que fez a solicitaç ão, a origem da solicitação e o número da porta da solicitaç ão do visualizador. Esses logs são úteis para aplicações como auditorias de segurança e acesso e investigação forense. Essa regra deve ser aplicada na região leste dos EUA-1.
7496	cloudwatch-log-group-encryp ted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptogra fia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	AWS Regra de configuração	Orientação
7496	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.
7496	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultad as.

ID de controle	AWS Regra de configuração	Orientação
7496	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o NZISM.

Práticas recomendadas operacionais para o PCI DSS 3.2.1

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 e as regras gerenciadas do AWS Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles PCI DSS. Um controle do PCI

DSS pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especificamente qualquer outro tráfego.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.		Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	autoscaling-launch-config-public-ip-disabled	Se você configura r suas interfaces de rede com um endereço IP público, os recursos associado s a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencion al a aplicações ou servidores.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicame nte. As instância s de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráv eis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicame nte. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicame nte. Os nós principai s do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	ec2-instances-in-vpc	Implemente instância s do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicaç ão segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadam ente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearc h Service dentro de um Amazon VPC permite a comunicaç ão segura entre o Amazon OpenSearc h Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	s3-account-level-p ublic-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	s3-bucket-level-pu blic-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.2.1	Restrinja o tráfego de entrada e de saída apenas ao necessário para o ambiente de dados do titular do cartão e negue especific amente qualquer outro tráfego.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3	Proíba o acesso público direto entre a Internet e qualquer componente do sistema no ambiente de dados do titular do cartão.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearc h de serviço em uma Amazon VPC permite a comunicaç ão segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolos e portas acessíveis publicamente que sejam autorizados.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.1	Implemente uma DMZ para limitar o tráfego de entrada apenas a componentes do sistema que fornecem serviços, protocolo s e portas acessívei s publicamente que sejam autorizados.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.2	Limite o tráfego de entrada da Internet aos endereços IP dentro da DMZ.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencion al em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantind o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicame nte. Essa regra ajuda a manter os dados confidenc iais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalm ente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuck ets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.4	Não permita o tráfego de saída não autorizado do ambiente de dados do titular do cartão para a Internet.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	netfw-policy-rule-group-associated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	netfw-stateless-rule-group-not-empty	Um grupo de regras do AWS Network Firewall contém regras que definem como seu firewall processa o tráfego em sua VPC. Um grupo de regras sem estado vazio, quando presente em uma política de firewall, não processa o tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque component es do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
1.3.6	Coloque component es do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque component es do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.3.6	Coloque component es do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositi vos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
1.3.6	Coloque componentes do sistema que armazenam dados do titular do cartão (como um banco de dados) em uma zona de rede interna, segregada da DMZ e de outras redes não confiáveis.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedido s pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacion ais, software que fornece serviços de segurança, contas de aplicativ os e sistemas, terminais point-of-sale (POS), aplicativ os de pagamento, cadeias de caractere s comunitárias do Simple Network Management Protocol (SNMP) etc.).	rds-cluster-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedido s pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacion ais, software que fornece serviços de segurança, contas de aplicativ os e sistemas, terminais point-of-sale (POS), aplicativ os de pagamento, cadeias de caractere s comunitárias do Simple Network Management Protocol (SNMP) etc.).	rds-instance-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de sua(s) instância(s) de banco de dados do Amazon Relational Database Service (Amazon RDS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedidos pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacionais, software que fornece serviços de segurança, contas de aplicativos e sistemas, terminais point-of-sale (POS), aplicativos de pagamento, cadeias de caracteres comunitárias do Simple Network Management Protocol (SNMP) etc.).	redshift-default-admin-check	Como os nomes de usuário padrão são de conhecimento público, a alteração dos nomes de usuário padrão pode ajudar a reduzir a superfície de ataque de seu(s) cluster(s) do Amazon Redshift.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedido s pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacion ais, software que fornece serviços de segurança, contas de aplicativ os e sistemas, terminais point-of-sale (POS), aplicativ os de pagamento, cadeias de caractere s comunitárias do Simple Network Management Protocol (SNMP) etc.).	redshift-default-db-name-check	Os nomes padrão são de conhecimento público e devem ser alterados durante a configuração. Alterar o nome do banco de dados padrão do cluster do Amazon Redshift pode ajudar a reduzir a superfície de ataque do cluster do Redshift.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedidos pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacionais, software que fornece serviços de segurança, contas de aplicativos e sistemas, terminais point-of-sale (POS), aplicativos de pagamento, cadeias de caracteres comunitárias do Simple Network Management Protocol (SNMP) etc.).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.1	Sempre altere os padrões concedido s pelo fornecedor e remova ou desative contas padrão desnecessárias antes de instalar um sistema na rede. Isso se aplica a TODAS as senhas padrão, incluindo, mas não se limitando às usadas por sistemas operacion ais, software que fornece serviços de segurança, contas de aplicativ os e sistemas, terminais point-of-sale (POS), aplicativ os de pagamento, cadeias de caractere s comunitárias do Simple Network Management Protocol (SNMP) etc.).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	ec2-instance-multiple-eni-check	Essa regra verifica se suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) têm vários ENIs. Ter vários ENIs pode causar instâncias com hospedagem dupla, ou seja, instâncias com várias sub-redes. Isso pode aumentar a complexidade da segurança da rede e introduzir caminhos e acessos de rede não intencionais.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: “Center for Internet Security (CIS)” “International Organization for Standardization (ISO) “ SysAdmin Audit Network Security (SANS) Institute of Standards Technology (NIST)”.	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: “Center for Internet Security (CIS)” “International Organization for Standardization (ISO) “ SysAdmin Audit Network Security (SANS) Institute of Standards Technolog y (NIST)”.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecidas e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2	Desenvolva padrões de configuração para todos os componentes do sistema. Verifique se esses padrões abordam todas as vulnerabilidades de segurança conhecida s e estão de acordo com padrões de proteção do sistema aceitos pelo setor. As fontes de padrões de fortalecimento do sistema aceitos pelo setor podem incluir, mas não estão limitadas a: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) • National Institute of Standards Technology (NIST).	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes component es do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.2	Habilite apenas serviços, protocolos, daemons etc. necessários para o funcionamento do sistema.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.2.3	Implemente recursos de segurança adicionais para quaisquer serviços, protocolos ou daemons necessários que sejam considerados inseguros.	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.3	Criptografe todo o acesso administr ativo que não seja do console usando criptografia forte.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
2.3	Criptografe todo o acesso administr ativo que não seja do console usando criptografia forte.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.3	Criptografe todo o acesso administr ativo que não seja do console usando criptografia forte.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
2.3	Criptografe todo o acesso administr ativo que não seja do console usando criptografia forte.	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
2.3	Criptografe todo o acesso administr ativo que não seja do console usando criptografia forte.	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Mantenha um inventário dos componentes do sistema que estão no escopo do PCI DSS.	ec2-security-group-attached-to-eni-periodic	Essa regra garante que os grupos de segurança sejam anexados a uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou a uma ENI. Essa regra ajuda a monitorar grupos de segurança não utilizados no inventário e no gerenciamento do seu ambiente.
2.4	Mantenha um inventário dos componentes do sistema que estão no escopo do PCI DSS.	eip-attached	Essa regra garante que os IPs elásticos alocados ao Amazon Virtual Private Cloud (Amazon VPC) sejam anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) ou às interfaces de rede elástica em uso. Essa regra ajuda a monitorar EIPs não utilizados em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Mantenha um inventário dos componentes do sistema que estão no escopo do PCI DSS.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
2.4	Mantenha um inventário dos componentes do sistema que estão no escopo do PCI DSS.	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	Reduza ao mínimo o armazenamento de dados do titular do cartão, implement ando políticas, procedimentos e processos de retenção e descarte de dados que incluam pelo menos o seguinte para todo o armazenamento de dados do titular do cartão (cardholder data, CHD): • Limite a quantidade de armazenamento de dados e o tempo de retenção ao necessári o para fins legais e regulatórios e/ou requisitos comerciais • Requisitos específic os de retenção para dados do titular do cartão • Processos para exclusão segura de dados quando não forem mais necessári os • Um processo trimestral para identificar e excluir com segurança dados	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	armazenados do titular do cartão que excedam a retenção definida.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	Reduza ao mínimo o armazenamento de dados do titular do cartão, implementando políticas, procedimentos e processos de retenção e descarte de dados que incluam pelo menos o seguinte para todo o armazenamento de dados do titular do cartão (cardholder data, CHD): • Limite a quantidade de armazenamento de dados e o tempo de retenção ao necessário para fins legais e regulatórios e/ou requisitos comerciais • Requisitos específicos de retenção para dados do titular do cartão • Processos para exclusão segura de dados quando não forem mais necessários • Um processo trimestral para identificar e excluir com segurança dados	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	armazenados do titular do cartão que excedam a retenção definida.		os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	Reduza ao mínimo o armazenamento de dados do titular do cartão, implementando políticas, procedimentos e processos de retenção e descarte de dados que incluam pelo menos o seguinte para todo o armazenamento de dados do titular do cartão (cardholder data, CHD): • Limite a quantidade de armazenamento de dados e o tempo de retenção ao necessário para fins legais e regulatórios e/ou requisitos comerciais • Requisitos específicos de retenção para dados do titular do cartão • Processos para exclusão segura de dados quando não forem mais necessários • Um processo trimestral para identificar e excluir com segurança dados	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	armazenados do titular do cartão que excedam a retenção definida.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1	Reduza ao mínimo o armazenamento de dados do titular do cartão, implement ando políticas, procedimentos e processos de retenção e descarte de dados que incluam pelo menos o seguinte para todo o armazenamento de dados do titular do cartão (cardholder data, CHD): • Limite a quantidade de armazenamento de dados e o tempo de retenção ao necessári o para fins legais e regulatórios e/ou requisitos comerciais • Requisitos específic os de retenção para dados do titular do cartão • Processos para exclusão segura de dados quando não forem mais necessári os • Um processo trimestral para identificar e excluir com segurança dados	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	armazenados do titular do cartão que excedam a retenção definida.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusive em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidirecionais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamento (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativamente trivial para um indivíduo mal-intencionado reconstruir os	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusive em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidirecionais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamento (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativamente trivial para um indivíduo mal-intencionado reconstruir os	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusive em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidirecionais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamento (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativamente trivial para um indivíduo mal-intencionado reconstruir os	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	sagemaker-endpoint -configuration-kms- key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.4	Torne o PAN ilegível em qualquer lugar onde ele esteja armazenado (inclusiv e em mídia digital portátil, mídia de backup e em logs) usando qualquer uma das seguintes abordagens: • Hashes unidireci onais baseados em criptografia forte (o hash deve ser de todo o PAN) • Truncamen to (o hash não pode ser usado para substituir o segmento truncado do PAN) • Tokens de índice e pads (os pads devem ser armazenados com segurança) • Criptografia forte com processos e procedimentos de gerenciamento de chaves associados. Observação: é um esforço relativam ente trivial para um indivíduo mal-inten cionado reconstruir os	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	dados PAN originais se tiver acesso à versão truncada e com hash de um PAN. Quando versões com hash e truncadas do mesmo PAN estiverem presentes no ambiente de uma entidade, devem ser implementados controles adicionais para garantir que as versões com hash e truncadas não possam ser correlacionadas para reconstruir o PAN original.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2	Restrinja o acesso às chaves criptográficas ao menor número necessário de responsáveis.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.2	Restrinja o acesso às chaves criptográficas ao menor número necessário de responsáveis.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Armazene sempre as chaves secretas e privadas usadas para criptografar/descriptografar dados do titular do cartão em um (ou mais) dos seguintes formulários: • Criptografado com uma chave de criptografia de chave que seja pelo menos tão forte quanto a chave de criptografia de dados e que seja armazenada separadamente da chave de criptografia de dados • Em um dispositivo criptográfico seguro (como um módulo de segurança de hardware (host) (HSM) ou point-of-interaction dispositivo aprovado pelo PTS) • Como em pelo menos dois componentes chave completos ou compartilhamentos de chaves, de acordo com um método aceito pelo setor.	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Nota: Não é necessário que as chaves públicas sejam armazenadas em um dos essas formas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Armazene sempre as chaves secretas e privadas usadas para criptografar/descriptografar dados do titular do cartão em um (ou mais) dos seguintes formulários: • Criptografado com uma chave de criptografia de chave que seja pelo menos tão forte quanto a chave de criptografia de dados e que seja armazenada separadamente da chave de criptografia de dados • Em um dispositivo criptográfico seguro (como um módulo de segurança de hardware (host) (HSM) ou point-of-interaction dispositivo aprovado pelo PTS) • Como em pelo menos dois componentes chave completos ou compartilhamentos de chaves, de acordo com um método aceito pelo setor.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Nota: Não é necessário que as chaves públicas sejam armazenadas em um dos essas formas.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5.3	Armazene sempre as chaves secretas e privadas usadas para criptografar/descriptografar dados do titular do cartão em um (ou mais) dos seguintes formulários: • Criptografado com uma chave de criptografia de chave que seja pelo menos tão forte quanto a chave de criptografia de dados e que seja armazenada separadamente da chave de criptografia de dados • Em um dispositivo criptográfico seguro (como um módulo de segurança de hardware (host) (HSM) ou point-of-interaction dispositivo aprovado pelo PTS) • Como em pelo menos dois componentes chave completos ou compartilhamentos de chaves, de acordo com um método aceito pelo setor.	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Nota: Não é necessário que as chaves públicas sejam armazenadas em um dos essas formas.		
3.6.4	Mudanças de chave criptográfica para chaves que chegaram ao final de seu criptoperíodo (por exemplo, após um período definido e/ou após uma certa quantidade de texto cifrado ter sido produzida por determinada chave), conforme definido pelo fornecedor de aplicações associado ou proprietário da chave e com base nas práticas recomendadas e diretrizes do setor (por exemplo, Publicação Especial NIST 800-57).	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.5	Retirada ou substituição (por exemplo, arquivamento, destruição e/ou revogação) de chaves conforme considerado necessário quando a integridade da chave tiver sido enfraquecida (por exemplo, saída de um funcionário com conhecimento de um componente chave em texto não criptografado), ou quando há suspeita de que as chaves estão comprometidas. Observação: se chaves criptográficas retiradas ou substituídas precisarem ser retidas, essas chaves deverão ser arquivadas com segurança (por exemplo, usando uma chave de criptografia). As chaves criptográficas arquivadas devem ser usadas apenas para fins de descriptografia/verificação.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.6.7	Prevenção de substituição não autorizada de chaves criptográficas.	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	acm-certificate-ex piration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	opensearch-https-r equired	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifiqu e-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearc h Service esteja ativada. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptogra fia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.1	Use criptografia forte e protocolos de segurança para proteger dados confidenciais do titular do cartão durante a transmiss ão em redes públicas abertas, incluindo o seguinte: • Somente chaves e certifica dos confiáveis são aceitos. • O protocolo em uso é compatível apenas com versões ou configurações seguras. • A força da criptografia é apropriada para a metodologia de criptografia em uso. Exemplos de redes públicas abertas incluem, mas não estão limitados a: • A Internet • Tecnologi as sem fio, incluindo 802.11 e Bluetooth • Tecnologias celulares, como Sistema Global para Comunicaç ões Móveis (GSM), Acesso Múltiplo por	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	Divisão de Código (CDMA) • Serviço Geral de Pacotes de Rádio (GPRS) • Comunicações via satélite		
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	elastic-beanstalk-managed-updates-en abled	Habilitar atualizaç ões gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções , atualizações e recursos de plataform a disponíveis para o ambiente sejam instalados. Uma das práticas recomenda das para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	ec2-managedinstanc e-association-comp liance-status-check	Use o AWS Systems Manager Associati ons para ajudar no inventário de plataformas e aplicativ os de software em uma organização. AWS O Systems Manager atribui um estado de configura ção às suas instância s gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacion al, instalações de software, configura ções de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	ec2-managedinstanc e-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	ecs-fargate-latest-platform-version	Atualizações e patches de segurança são implantados automaticamente para suas tarefas do AWS Fargate. Se for encontrad o um problema de segurança que afete uma versão da plataforma AWS Fargate, AWS corrija a versão da plataform a. Para ajudar no gerenciamento de patches de suas tarefas do Amazon Elastic Container Service (ECS) executando o AWS Fargate, atualize as tarefas autônomas de seus serviços para usar a versão mais recente da plataform a.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	rds-automatic-mino r-version-upgrade-enabled	Habilite atualizaç ões automáticas de versões secundári as nas instâncias do Amazon Relationa l Database Service (RDS) para garantir que as últimas atualizações de versões secundári as do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.2	Verifique se todos os component es do sistema e o software estão protegidos contra vulnerabilidades conhecidas instalando patches de segurança aplicáveis concedido s pelo fornecedor. Instale patches de segurança críticos em até um mês após o lançament o. Observação: os patches críticos de segurança devem ser identificados de acordo com o processo de classific ação de risco definido no Requisito 6.1.	redshift-cluster-m aintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configura ções preferidas da organização. Especificamente, que eles tenham janelas de manutençã o preferenciais e períodos automatiz ados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrad e o. O padrão é true. Também permite definir opcionalmente o preferredMaintenan ceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3.2	Revise o código personalizado antes de liberá-lo para produção ou clientes, a fim de identificar qualquer vulnerabi lidade potencial de codificação (usando processos manuais ou automatizados) para incluir pelo menos o seguinte: • As alterações no código são revisadas por indivíduos que não sejam o autor do código de origem e por indivíduos cientes de técnicas de revisão de código e práticas de codificaç ão segura. • As revisões de código garantem que o código seja desenvolv ido de acordo com as diretrizes de codificaç ão segura. • As correções apropriadas são implementadas antes do lançament o. • Os resultados da revisão do código	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner . Habilitar a verificaç ão de imagens em repositórios do ECR adiciona uma camada de verificaç ão da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	são analisados e aprovados pela administração antes da divulgação. (Continua na próxima página)		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	alb-desync-mode-check	Para ajudar na proteção de aplicações contra vulnerabilidades de dessincronização de HTTP, habilite o modo de mitigação de dessincronização de HTTP nos Application Load Balancers. Problemas de dessincronização de HTTP podem levar ao contrabando de solicitações e tornar suas aplicações vulneráveis ao envenenamento da fila de solicitações ou do cache. Os modos de mitigação de dessincronização são: monitorado, defensivo e mais rigoroso. Ddefensivo é o modo padrão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicaçõe s web voltadas ao público, para verificar continuamente todo o tráfego.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicaçõe s web voltadas ao público, para verificar continuamente todo o tráfego.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicaçõe s web voltadas ao público, para verificar continuamente todo o tráfego.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicações web voltadas ao público, para verificar continuamente todo o tráfego.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicaçõe s web voltadas ao público, para verificar continuamente todo o tráfego.		

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.6	Para aplicações web voltadas ao público, aborde novas ameaças e vulnerabilidades continuamente e garanta que essas aplicações estejam protegidas contra ataques conhecidos por um dos seguintes métodos: • Revisão de aplicações web voltadas ao público por meio de ferramentas ou métodos manuais ou automatizados de avaliação de segurança de vulnerabilidades de aplicações, ao menos a cada e após qualquer alteração. Observação: esta avaliação não é a mesma que as verificações de vulnerabilidade realizadas para o Requisito 11.2. • Instalar uma solução técnica automatizada que detecte	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
	e impeça ataques baseados na web (por exemplo, um firewall de aplicações web) na frente de aplicações web voltadas ao público, para verificar continuamente todo o tráfego.		
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
7.1.1	Defina as necessida des de acesso para cada função, incluindo : • Component es do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessári o (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.1	Defina as necessidades de acesso para cada função, incluindo: • Componentes do sistema e recursos de dados que cada função precisa acessar para sua função de trabalho. • Nível de privilégio necessário (por exemplo, usuário, administrador etc.) para acessar recursos.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedAc tionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decry pt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessári os para executar as responsabilidades do trabalho.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários para executar as responsabilidades do trabalho.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários os para executar as responsabilidades do trabalho.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.1.2	Restrinja o acesso a IDs de usuários privilegiados aos privilégios mínimos necessários para executar as responsabilidades do trabalho.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringe m o acesso com base nas informaçõ es essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.1	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: cobertura de todos os componentes do sistema.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	ecs-containers-nonprivileged	Para ajudar na implementação do princípio de privilégio mínimo, as definições de tarefas do Amazon Elastic Container Service (Amazon ECS) não devem ter o privilégio elevado habilitado. Quando esse parâmetro é verdadeiro, o contêiner recebe privilégios elevados na instância de contêiner host (semelhante ao usuário raiz).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	ecs-containers-readonly-access	Habilitar o acesso somente de leitura aos contêineres do Amazon Elastic Container Service (ECS) pode ajudar a aderir à entidade principal de privilégio mínimo. Essa opção pode reduzir os vetores de ataque, pois o sistema de arquivos da instância do contêiner não pode ser modificado, a menos que tenha permissões explícitas de leitura e gravação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizações de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			políticas da organizaç ão.
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringe m o acesso com base nas informaçõ es essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégi os a indivíduos com base na classificação e função do cargo.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms:From). ReEncrypt Os

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			valores reais devem refletir as políticas da organização.
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.2	Estabeleça sistemas de controle de acesso para componentes do sistema que restringem o acesso com base nas informações essenciais de um usuário e que sejam definidos como "negar tudo", a menos que haja uma permissão específica. Esses sistemas de controle de acesso devem incluir o seguinte: atribuição de privilégios a indivíduos com base na classificação e função do cargo.	opensearch-access-control-enabled	Garanta que o controle de acesso refinado esteja ativado em seus domínios do Amazon OpenSearch Service. O controle de acesso refinado fornece mecanismos de autorização aprimorados para obter acesso menos privilegiado aos domínios do Amazon Service. OpenSearch Ele permite o controle de acesso baseado em funções ao domínio, bem como segurança em nível de índice, documento e campo, suporte para multilocação de painéis de OpenSearch serviço e autenticação básica HTTP para Service e Kibana. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
7.2.3	Configuração padrão “negar tudo”.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1.1	Atribua a todos os usuários uma ID exclusiva antes de permitir que eles acessem os componentes do sistema ou os dados do titular do cartão.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1.4	Remova/desative contas de usuários inativas em 90 dias.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	codebuild-project-environment-privil eged-check	Para ajudar na implementação do princípio do menor privilégio, certifique-se de que seu ambiente de CodeBuild projeto da Amazon não tenha o modo privilegi ado ativado. Essa configuração deve ser desabilitada para evitar o acesso não intencional às APIs do Docker, bem como ao hardware subjacente do contêiner.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	ecs-no-environment-secrets	Como prática recomendada de segurança, passe informaçõ es confidenciais para contêineres como variáveis de ambiente. Você pode injetar dados com segurança em seus contêineres do Amazon Elastic Container Service (ECS) referenciando valores armazenad os no AWS Systems Manager Parameter Store ou no Secrets Manager AWS na definição de contêiner de uma definição de tarefa do Amazon ECS. Em seguida, é possível expor suas informações confidenciais como variáveis de ambiente ou na configuração de log de um contêiner.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenciais em repouso nesses volumes, habilite a criptografia em repouso para ajudar a protegê-los.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	elasticsearch-encr ypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service).
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	opensearch-encrypt ed-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	rds-snapshot-encry pted	Habilite a criptogra fia para os snapshots do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instâncias do Amazon Relationa l Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instância s do Amazon RDS, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	redshift-cluster-c onfiguration-check	Para proteger os dados em repouso, habilite a criptogra fia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	s3-bucket-ssl-requ ests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenc iais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	sagemaker-notebook -instance-kms-key- configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker notebook. Como dados confidenc iais podem existir em repouso no SageMaker notebook, ative a criptografia em repouso para ajudar a proteger esses dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	secretsmanager-usi ng-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.1	Uso de criptografia forte, renderização de todas as credencia is de autenticação (como senhas/frases) ilegíveis durante a transmissão e armazenamento em todos os component es do sistema.	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptogra fia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenc iais em repouso em mensagens publicada s, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.3	As senhas/frases secretas devem atender ao seguinte: • Exigir um comprimento mínimo de pelo menos sete caracteres. • Conter caracteres numéricos e alfabéticos. Como alternativa, as senhas/frases secretas devem ter complexidade e força ao menos equivalentes aos parâmetros especificados acima.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (padrão do PCI DSS: falso), RequireLowercaseCharacters (padrão do PCI DSS: verdadeiro), (padrão do PCI DSS: falso), RequireSymbols (padrão do PCI DSS: verdadeiro), RequireNumbers (padrão do PCI DSS: 7), MinimumPasswordLength (padrão do PCI DSS: 4) e

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			PasswordReusePreve ntion MaxPasswo rdAge (padrão do PCI DSS: 90) para sua política de senha do IAM. Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.4	Altere as senhas/ frases secretas do usuário pelo menos a cada 90 dias.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.4	Altere as senhas/ frases secretas do usuário pelo menos a cada 90 dias.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (padrão do PCI DSS: falso), RequireLowercaseCharacters (padrão do PCI DSS: verdadeiro), (padrão do PCI DSS: falso), RequireSymbols (padrão do PCI DSS: verdadeiro), RequireNumbers (padrão do PCI DSS: 7), MinimumPasswordLength (padrão do PCI DSS: 4) e

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			PasswordReusePreve ntion MaxPasswo rdAge (padrão do PCI DSS: 90) para sua política de senha do IAM. Os valores reais devem refletir as políticas da organizaç ão.
8.2.4	Altere as senhas/ frases secretas do usuário pelo menos a cada 90 dias.	secretsmanager-rot ation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternânc ia de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.2.5	Não permita que um indivíduo envie uma nova senha/frase secreta que seja igual a qualquer uma das últimas quatro senhas/frases secretas que ele ou ela usou.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (padrão do PCI DSS: falso), RequireLowercaseCharacters (padrão do PCI DSS: verdadeiro), (padrão do PCI DSS: falso), RequireSymbols (padrão do PCI DSS: verdadeiro), RequireNumbers (padrão do PCI DSS: 7), MinimumPasswordLength (padrão do PCI DSS: 4) e

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			PasswordReusePreve ntion MaxPasswo rdAge (padrão do PCI DSS: 90) para sua política de senha do IAM. Os valores reais devem refletir as políticas da organizaç ão.
8.3.1	Incorpore a autentica ção multifator para todos os acessos que não são do console no CDE para pessoal com acesso administr ativo.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas compromet idas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.1	Incorpore a autenticação multifator para todos os acessos que não são do console no CDE para pessoal com acesso administrativo.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.1	Incorpore a autenticação multifator para todos os acessos que não são do console no CDE para pessoal com acesso administrativo.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.1	Incorpore a autenticação multifator para todos os acessos que não são do console no CDE para pessoal com acesso administrativo.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.2	Incorpore a autenticação multifatorial para todos os acessos remotos à rede (tanto de usuário quanto de administrador, incluindo acesso de terceiros para suporte ou manutenção) originados de fora da rede da entidade.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.2	Incorpore a autenticação multifatorial para todos os acessos remotos à rede (tanto de usuário quanto de administrador, incluindo acesso de terceiros para suporte ou manutenção) originados de fora da rede da entidade.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.2	Incorpore a autenticação multifatorial para todos os acessos remotos à rede (tanto de usuário quanto de administrador, incluindo acesso de terceiros para suporte ou manutenção) originados de fora da rede da entidade.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.3.2	Incorpore a autenticação multifatorial para todos os acessos remotos à rede (tanto de usuário quanto de administrador, incluindo acesso de terceiros para suporte ou manutenção) originados de fora da rede da entidade.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além do nome de usuário e senha. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.1	Implemente trilhas de auditoria para vincular todo o acesso aos componentes do sistema a cada usuário individual.	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.1	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstituir os seguintes eventos: todos os acessos de usuários individuais aos dados do titular do cartão	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.2	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: todas as ações realizadas por qualquer pessoa com privilégios raiz ou administrativos	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.3	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: acesso a todas as trilhas de auditoria	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.4	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: tentativas de acesso lógico inválidas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.5	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: uso de e alterações nos mecanismos de identificação e autenticação — incluindo, dentre outros, a criação de novas contas e a elevação de privilégios — e todas as alterações, adições ou exclusões em contas com privilégios raiz ou administrativos	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.6	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: inicialização, interrupção ou pausa dos logs de auditoria	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.6	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: inicialização, interrupção ou pausa dos logs de auditoria	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.6	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: inicialização, interrupção ou pausa dos logs de auditoria	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Management Console e as chamadas de API. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD_TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.2.7	Implemente trilhas de auditoria automatizadas para todos os componentes do sistema a fim de reconstruir os seguintes eventos: criação e exclusão de objetos no nível do sistema	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernéti ca. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.3.1	Registre pelo menos as seguintes entradas da trilha de auditoria para todos os componentes do sistema de cada evento: identificação do usuário	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5	Proteja trilhas de auditoria para que não possam ser alteradas.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.
10.5	Proteja trilhas de auditoria para que não possam ser alteradas.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5	Proteja trilhas de auditoria para que não possam ser alteradas.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.
10.5.2	Proteja arquivos de trilha de auditoria contra modificações não autorizadas.	cloud-trail-encryption-enabled	Como podem existir dados confidenc iais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitada para suas AWS CloudTrail trilhas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5.2	Proteja arquivos de trilha de auditoria contra modificações não autorizadas.	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptogra fia para ajudar a protegê-los.
10.5.2	Proteja arquivos de trilha de auditoria contra modificações não autorizadas.	s3-default-encryption-kms	Habilite a criptogra fia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5.3	Faça backup imediatamente dos arquivos de trilha de auditoria em um servidor de log centralizado ou em mídia que seja difícil de alterar.	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5.3	Faça backup imediatamente dos arquivos de trilha de auditoria em um servidor de log centralizado ou em mídia que seja difícil de alterar.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
10.5.3	Faça backup imediatamente dos arquivos de trilha de auditoria em um servidor de log centralizado ou em mídia que seja difícil de alterar.	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
10.5.3	Faça backup imediatamente dos arquivos de trilha de auditoria em um servidor de log centralizado ou em mídia que seja difícil de alterar.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5.5	Use software de monitoramento de integridade de arquivo ou detecção de alterações em logs para garantir que os dados de log existentes não possam ser alterados sem gerar alertas (embora novos dados adicionados não devam causar um alerta).	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integrida de dos CloudTrail registros. A validação do arquivo de log ajuda a determina r se um arquivo de log foi modificado, excluído ou inalterad o após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computaci onalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.5.5	Use software de monitoramento de integridade de arquivo ou detecção de alterações em logs para garantir que os dados de log existentes não possam ser alterados sem gerar alertas (embora novos dados adicionados não devam causar um alerta).	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.7	Retenha o histórico da trilha de auditoria por ao menos um ano, com um mínimo de três meses imediatamente disponíveis para análise (por exemplo, online, arquivado ou restaurável a partir de backup).	s3-lifecycle-policy-check	Configure as políticas de ciclo de vida do Amazon S3 para definir ações que você deseja que o Amazon S3 realize durante o ciclo de vida de um objeto (por exemplo, fazer a transição de objetos para outra classe de armazenamento, arquivá-los ou excluí-los após um período especificado).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
10.7	Retenha o histórico da trilha de auditoria por ao menos um ano, com um mínimo de três meses imediatamente disponíveis para análise (por exemplo, online, arquivado ou restaurável a partir de backup).	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
11.2.3	Execute verificações internas e externas e verifique novamente conforme necessário, após qualquer alteração significativa. As verificações devem ser realizadas por pessoal qualificado.	ecr-private-image-scanning-enabled	A verificação de imagem do Amazon Elastic Container Repository (ECR) ajuda a identificar vulnerabilidades de software nas imagens do contêiner. Habilitar a verificação de imagens em repositórios do ECR adiciona uma camada de verificação da integridade e segurança das imagens que estão sendo armazenadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Use técnicas de detecção e/ou prevenção de intrusões para detectar e/ou prevenir invasões na rede. Monitore todo o tráfego no perímetro do ambiente de dados do titular do cartão, bem como em pontos críticos do ambiente de dados do titular do cartão, e alerte o pessoal sobre suspeitas de comprometimento. Mantenha todos os mecanismos, linhas de base e assinatur as de detecção e prevenção de invasões atualizados.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.4	Use técnicas de detecção e/ou prevenção de intrusões para detectar e/ou prevenir invasões na rede. Monitore todo o tráfego no perímetro do ambiente de dados do titular do cartão, bem como em pontos críticos do ambiente de dados do titular do cartão, e alerte o pessoal sobre suspeitas de comprometimento. Mantenha todos os mecanismos, linhas de base e assinatur as de detecção e prevenção de invasões atualizados.	netfw-policy-rule-group-associated	Uma política AWS de firewall de rede define como seu firewall monitora e gerencia o tráfego em uma Amazon VPC. Você configura grupos de regras stateless e stateful para filtrar pacotes e fluxos de tráfego e define o tratamento padrão do tráfego.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.5	Implemente um mecanismo de detecção de alterações (por exemplo, ferramentas de monitoramento de integridade de arquivos) para alertar o pessoal sobre modificações não autorizadas (incluindo alterações, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configure o software para realizar comparações de arquivos críticos ao menos uma vez por semana.	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificado, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrail falsificar arquivos de log sem detecção.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
11.5	Implemente um mecanismo de detecção de alterações (por exemplo, ferramentas de monitoramento de integridade de arquivos) para alertar o pessoal sobre modificações não autorizadas (incluindo alterações, adições e exclusões) de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo; e configure o software para realizar comparações de arquivos críticos ao menos uma vez por semana.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros . AWS

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para PCI DSS 3.2.1.

Práticas recomendadas operacionais para recursos acessíveis ao público

Esse pacote de conformidade ajuda a identificar recursos que podem estar acessíveis ao público.

Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para recursos acessíveis ao público.

Práticas recomendadas operacionais para a estrutura de segurança cibernética do RBI para UCBs

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre a Estrutura de Segurança Cibernética do Banco da Reserva da Índia (RBI) para bancos cooperativos urbanos (UCBs) e as regras gerenciadas do AWS Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do RBI Cyber Security Framework para UCBs. Uma estrutura de segurança cibernética do RBI para controle de UCBs pode estar relacionada a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.1)	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para

ID de controle	AWS Regra de configuração	Orientação
		fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
Anexo_I (1.1)	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsistências nas configurações da conta, o que pode expor recursos e dados confidenciais.
Anexo_I (1.1)	ecr-private-tag-immutability-enabled	Habilite a imutabilidade de tags do Elastic Container Repository (ECR) para evitar que as tags de imagem em suas imagens do ECR sejam sobrescritas. Anteriormente, as tags podiam ser substituídas, exigindo metodologias manuais para identificar uma imagem de forma exclusiva.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantind o que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
Anexo_I (1.3)	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo_I (1.3)	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecione automaticamente as solicitaç ões HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	api-gw-cache-enabled-and-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para o cache do estágio do API Gateway. Como dados confidenciais podem ser capturados para o método da API, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
Anexo_I (1.3)	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitações.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo_I (1.3)	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
Anexo_I (1.3)	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	backup-recovery-point-encrypted	Certifique-se de que a criptografia esteja ativada para seus pontos AWS de recuperação de Backup. Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	codebuild-project-artifact-encryption	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild artefatos.
Anexo_I (1.3)	codebuild-project-s3-logs-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus AWS CodeBuild registros armazenados no Amazon S3.
Anexo_I (1.3)	opensearch-encrypted-at-rest	Como dados confidenciais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch Service.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
Anexo_I (1.3)	opensearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo_I (1.3)	dynamodb-table-encrypted-kms	Habilite a criptografia para as tabelas do Amazon DynamoDB. Como pode haver dados confidenc iais em repouso nessas tabelas, habilite a criptogra fia em repouso para ajudar a protegê-los. Por padrão, as tabelas do DynamoDB são criptografadas com AWS uma chave mestra de cliente (CMK) própria.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
Anexo_I (1.3)	elasticsearch-encrypted-at-rest	Como dados confidenc iais podem existir e para ajudar a proteger dados em repouso, assegure-se de que a criptografia esteja habilitada para seus domínios do Amazon OpenSearch OpenSearch Service (Service) .

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	elasticsearch-node-to-node-encryption-check	Certifique-se node-to-node de que a criptografia para o Amazon OpenSearch Service esteja ativada. A ode-to-no de criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da Amazon Virtual Private Cloud (Amazon VPC). Como pode haver dados confidenc iais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo_I (1.3)	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.
Anexo_I (1.3)	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptores SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
Anexo_I (1.3)	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
Anexo_I (1.3)	rds-snapshot-encrypted	Habilite a criptografia para os snapshots do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	rds-storage-encrypted	Para ajudar a proteger os dados em repouso, habilite a criptografia para as instância s do Amazon Relational Database Service (Amazon RDS). Como pode haver dados confidenciais em repouso nas instâncias do Amazon RDS, habilite a criptografia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
Anexo_I (1.3)	s3-bucket-server-side-encryption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
Anexo_I (1.3)	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	sagemaker-endpoint-configuration-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu SageMaker endpoint. Como dados confidenciais podem existir em repouso no SageMaker endpoint, ative a criptografia em repouso para ajudar a proteger esses dados.
Anexo_I (1.3)	sagemaker-notebook-instance-kms-key-configured	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitad a para seu SageMaker notebook. Como dados confidenciais podem existir em repouso no SageMaker notebook, ative a criptogra fia em repouso para ajudar a proteger esses dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.
Anexo_I (1.3)	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informaçõ es confidenciais, e o controle de acesso é necessário para essas contas.
Anexo_I (1.3)	ebs-snapshot-public-restora ble-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicame nte. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
Anexo_I (1.3)	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearc h serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenc iais, e o controle de acesso é necessário para essas contas.
Anexo_I (1.3)	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
Anexo_I (1.3)	no-unrestricted-route-to-igw	Garanta que as tabelas de rotas do Amazon EC2 não tenham rotas irrestritas para um gateway da Internet. Remover ou limitar o acesso à internet para workloads no Amazon VPC pode reduzir o acesso não intencional em seu ambiente.
Anexo_I (1.3)	redshift-cluster-kms-enabled	Para ajudar a proteger dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para seu cluster do Amazon Redshift. Como pode haver dados confidenciais em repouso nos clusters do Redshift, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.
Anexo_I (1.3)	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instâncias do Amazon Elastic Compute Cloud (EC2) que são executadas em sub-redes com esse atributo habilitado têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
Anexo_I (1.3)	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
Anexo_I (1.3)	rds-snapshots-public-prohib ited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instância s do Amazon Relational Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informações confidenc iais e princípios, e o controle de acesso é necessário para essas contas.
Anexo_I (1.3)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.
Anexo_I (1.3)	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (1.3)	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
Anexo_I (1.3)	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
Anexo_I (5.1)	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicações web. Um WAF ajuda a proteger aplicações web ou APIs contra explorações comuns da web. Essas explorações da web podem afetar a disponibilidade, comprometer a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (5.1)	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
Anexo_I (5.1)	waf-regional-rule-not-empty	Certifique-se de que seu AWS WAF tenha uma regra que não esteja vazia. Uma regra sem condições pode resultar em comportamento não intencional.
Anexo_I (5.1)	waf-regional-rulegroup-not-empty	Certifique-se de que seu AWS WAF tenha um grupo de regras que não esteja vazio. Um grupo de regras vazio pode resultar em um comportamento não intencion al.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (5.1)	waf-regional-webacl-not-empty	Uma Web ACL anexada a um AWS WAF pode conter uma coleção de regras e grupos de regras para inspecionar e controlar solicitações da web. Se uma ACL da web estiver vazia, o tráfego da web passará sem ser detectado ou acionado pelo WAF.
Anexo_I (5.1)	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (5.1)	api-gw-associated-with-waf	AWS O WAF permite que você configure um conjunto de regras (chamado de lista de controle de acesso à web (Web ACL)) que permite, bloqueia ou conta solicitações da web com base nas regras e condições de segurança da web personalizáveis que você define. Associe seu estágio do Amazon API Gateway a uma ACL da web do WAF para protegê-lo contra ataques mal-intencionados.
Anexo_I (5.1)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (5.1)	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPo rt1-blockedPort5 (Padrões de configuração: 20.21.338 9.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (6)	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.
Anexo_I (6)	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (6)	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.
Anexo_I (6)	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (6)	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relaciona l (RDBMS) estejam instalada s, o que pode incluir patches de segurança e correções de bugs.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (6)	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 - sat: 16:30) e o automated SnapshotRetention Período (o padrão é 1). Os valores reais devem refletir as políticas da organização.
Anexo_I (6)	vuln-management-plan-exists (verificação do processo)	Desenvolva e implemente um plano de gerenciamento de vulnerabilidades para ter um processo formalmente definido para lidar com as vulnerabilidades em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.1)	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso”: “*”. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
Anexo_I (7.1)	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.1)	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.
Anexo_I (7.1)	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.1)	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.2)	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
Anexo_I (7.3)	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
Anexo_I (7.4)	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.
Anexo_I (7.4)	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Managemen t Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
Anexo_I (7.4)	cloudtrail-s3-dataevents-en abled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo_I (7.4)	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identific ação de eventos possivelm ente mal-intencionados.
Anexo_I (7.4)	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informaçõ es detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitação foi recebida, o endereço IP do cliente, latências, caminhos de solicitação e respostas do servidor.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.
Anexo_I (7.4)	opensearch-audit-logging-enabled	Certifique-se de que o registro de auditoria esteja ativado em seus domínios OpenSearch do Amazon Service. O registro de auditoria permite que você acompanhe a atividade do usuário em seus OpenSearch domínios, incluindo sucessos e falhas de autenticação, solicitações, alterações de índice e consultas de pesquisa recebidas. OpenSearch

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
Anexo_I (7.4)	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail registra ações do AWS Managemen t Console e chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrail entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REGION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrail criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relational Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.
Anexo_I (7.4)	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
Anexo_I (7.4)	wafv2-logging-enabled	Para ajudar com o registro e o monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informações detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (7.4)	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessári as nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitad o para fornecer informações sobre conexões e atividade s do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEn abled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.
Anexo_I (10.2)	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscient ização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliência.
Anexo_I (12)	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado . Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.
Anexo_I (12)	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Anexo_I (12)	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir os requisitos da organização.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especificado pela organização. Os backups automáticos podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.
Anexo_I (12)	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.
Anexo_I (12)	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas . A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	AWS Regra de configuração	Orientação
Anexo_I (12)	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar , recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para a estrutura de segurança cibernética do RBI para UCBs.

Práticas recomendadas operacionais para o RBI MD-ITF

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

A seguir, é apresentado um exemplo de mapeamento entre a Direção Principal — Estrutura de Tecnologia da Informação do Banco da Reserva da Índia (RBI) e as regras AWS gerenciadas do Config. Cada regra do Config se aplica a um AWS recurso específico e está relacionada a um ou mais controles do RBI Master Direction — Information Technology Framework. Um controle da

Direção Principal, Estrutura de Tecnologia da Informação do RBI pode estar relacionado a várias regras do Config. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(a)	Identificação e classificação de ativos de informação.	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
3.1(a)	Identificação e classificação de ativos de informação.	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
3.1(a)	Identificação e classificação de ativos de informação.	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(a)	Identificação e classificação de ativos de informação.	ecr-private-tag-immutability-enabled	Habilite a imutabilidade de tags do Elastic Container Repository (ECR) para evitar que as tags de imagem em suas imagens do ECR sejam sobrescritas. Anteriormente, as tags podiam ser substituídas, exigindo metodologias manuais para identificar uma imagem de forma exclusiva.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
3.1(c)	Controle de acesso com base em função	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).
3.1(c)	Controle de acesso com base em função	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando as senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciam ento de privilégio mínimo e permissões.
3.1(c)	Controle de acesso com base em função	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessári as. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
3.1(c)	Controle de acesso com base em função	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(c)	Controle de acesso com base em função	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(g)	Gerenciamento de incidentes	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(g)	Gerenciamento de incidentes	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(g)	Gerenciamento de incidentes	alb-waf-enabled	Certifique-se de que o AWS WAF esteja ativado nos Elastic Load Balancers (ELB) para ajudar a proteger aplicativ os da web. Um WAF ajuda a proteger aplicações web ou APIs contra exploraçõ es comuns da web. Essas exploraçõ es da web podem afetar a disponibi lidade, compromet er a segurança ou consumir recursos excessivos em seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(g)	Gerenciamento de incidentes	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(g)	Gerenciamento de incidentes	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
3.1(h)	Trilhas	api-gw-execution-logging-enabled	O registro em log do API Gateway exibe visualizações detalhadas dos usuários que acessaram a API e a forma como eles a acessaram. Esse insight mostra as atividades do usuário.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
3.1(h)	Trilhas	codebuild-project-logging-enabled	Certifique-se de que o registro AWS CodeBuild do projeto esteja ativado para que seus registros de saída de compilação sejam enviados para a Amazon CloudWatch ou para o Amazon Simple Storage Service (Amazon S3). Os logs de saída de compilação fornecem informações detalhadas sobre o projeto de compilação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	opensearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. OpenSearch Os registros de erros do serviço podem ajudar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.
3.1(h)	Trilhas	redshift-audit-logging-enabled	Para capturar informações sobre conexões e atividades de usuários no cluster do Amazon Redshift, habilite o registro em log de auditoria.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identific ar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.
3.1(h)	Trilhas	cloudtrail-s3-data events-enabled	A coleta de eventos de dados do Simple Storage Service (Amazon S3) ajuda a detectar qualquer atividade anômala. Os detalhes incluem Conta da AWS informações que acessaram um bucket do Amazon S3, endereço IP e horário do evento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	cw-loggroup-retention-period-check	Uma duração mínima dos dados de log de eventos deve ser retida para os grupos de logs a fim de ajudar na solução de problemas e nas investigações forenses. A falta de dados de log de eventos anteriores disponíveis dificulta a reconstrução e a identificação de eventos possivelmente mal-intencionados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	elasticsearch-logs-to-cloudwatch	Certifique-se de que os domínios do Amazon OpenSearch Service tenham registros de erros habilitados e transmitidos para o Amazon CloudWatch Logs para retenção e resposta. Os logs de erros do domínio podem auxiliar nas auditorias de segurança e acesso, além de ajudar a diagnosticar problemas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	elb-logging-enabled	A atividade do Elastic Load Balancing é um ponto central de comunicação em um ambiente. Habilite o registro em log do ELB. Os dados coletados fornecem informações detalhadas sobre as solicitações enviadas ao ELB. Cada log contém informaçõ es como a hora em que a solicitaç ão foi recebida, o endereço IP do cliente, latências, caminhos de solicitaç ão e respostas do servidor.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	multi-region-cloudtrail-enabled	AWS CloudTrail registra as ações do AWS Managemen t Console e as chamadas de API. Você pode identific ar quais usuários e contas ligaram AWS, o endereço IP de origem de onde as chamadas foram feitas e quando elas ocorreram. CloudTrai l entregará arquivos de log de todas as AWS regiões para seu bucket do S3 se MULTI_REG ION_CLOUD _TRAIL_ENABLED estiver habilitado. Além disso, ao AWS lançar uma nova região, CloudTrai l criará a mesma trilha na nova região. Como resultado, você receberá arquivos de log contendo a atividade da API para a nova região sem realizar nenhuma ação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	rds-logging-enabled	Para ajudar no registro em log e no monitoramento em seu ambiente, habilite o registro em log do Amazon Relationa l Database Service (Amazon RDS). Com o registro em log do Amazon RDS, você pode capturar eventos como conexões, desconexões, consultas ou tabelas consultadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhados das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitação de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhados de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	wafv2-logging-enabled	Para ajudar no registro e no monitoramento em seu ambiente, habilite o registro do AWS WAF (V2) em ACLs da web regionais e globais. AWS O registro do WAF fornece informaçõ es detalhadas sobre o tráfego que é analisado pela sua ACL da web. Os registros registram a hora em que o AWS WAF recebeu a solicitação do seu AWS recurso, informações sobre a solicitação e uma ação para a regra à qual cada solicitação correspondeu.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(h)	Trilhas	redshift-cluster-configuration-check	Para proteger os dados em repouso, habilite a criptografia para os clusters do Amazon Redshift. Implante também as configurações necessárias nos clusters do Amazon Redshift. O registro em log de auditoria deve ser habilitado para fornecer informações sobre conexões e atividades do usuário no banco de dados. Essa regra exige que um valor seja definido para clusterDbEncrypted (Config Default: TRUE) e LoggingEnabled (Config Default: TRUE). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(i)	Infraestrutura de chave pública	acm-certificate-expiration-check	Garanta que a integridade da rede seja protegida garantindo que os certificados X509 sejam emitidos pelo AWS ACM. Esses certificados devem ser válidos e estar dentro do prazo de validade. Essa regra exige um valor para daysToExpiration (valor das melhores práticas de segurança AWS básicas: 90). O valor real deve refletir as políticas da organização.
3.1(i)	Infraestrutura de chave pública	alb-http-drop-invalid-header-enabled	Configure seus Elastic Load Balancers (ELB) para descartar cabeçalhos http. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(i)	Infraestrutura de chave pública	alb-http-to-https-redirection-check	Para ajudar a proteger os dados em trânsito, garanta que o Application Load Balancer redirecio ne automaticamente as solicitações HTTP não criptografadas para HTTPS. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1(i)	Infraestrutura de chave pública	api-gw-ssl-enabled	Configure os estágios da API REST do Amazon API Gateway com certificados SSL para permitir que os sistemas de back-end autentiquem o API Gateway como origem das solicitaç ões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(i)	Infraestrutura de chave pública	opensearch-https-required	Como dados confidenciais podem existir e para ajudar a proteger os dados em trânsito, certifique-se de que o HTTPS esteja habilitado para conexões com seus domínios do Amazon OpenSearch Service.
3.1(i)	Infraestrutura de chave pública	elbv2-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptografia para o Elastic Load Balancing. Use o AWS Certificate Manager para gerenciar, provisionar e implantar certificados SSL/TLS públicos e privados com AWS serviços e recursos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(i)	Infraestrutura de chave pública	elb-acm-certificate-required	Como pode haver dados confidenciais, e para ajudar a proteger os dados em trânsito, habilite a criptogra fia para o Elastic Load Balancing. Use o AWS Certifica te Manager para gerenciar, provision ar e implantar certifica dos SSL/TLS públicos e privados com AWS serviços e recursos internos.
3.1(i)	Infraestrutura de chave pública	elb-tls-https-listeners-only	Configure os Elastic Load Balancers (ELBs) com receptore s SSL ou HTTPS. Como pode haver dados confidenciais, habilite a criptogra fia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.1(i)	Infraestrutura de chave pública	redshift-require-tls-ssl	Os clusters do Amazon Redshift devem exigir criptografia TLS/SSL para se conectar aos clientes SQL. Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.
3.1(i)	Infraestrutura de chave pública	s3-bucket-ssl-requests-only	Para ajudar a proteger dados em trânsito, os buckets do Amazon Simple Storage Service (Amazon S3) devem exigir solicitações de uso do Secure Socket Layer (SSL). Como pode haver dados confidenciais, habilite a criptografia em trânsito para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	elastic-beanstalk-managed-updates-enabled	Habilitar atualizações gerenciadas da plataforma para um ambiente do Amazon Elastic Beanstalk garante que as últimas correções, atualizações e recursos de plataforma disponíveis para o ambiente sejam instalados. Uma das práticas recomendadas para proteger sistemas é manter a instalação de patches em dia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	rds-automatic-minor-version-upgrade-enabled	Habilite atualizações automáticas de versões secundárias nas instâncias do Amazon Relational Database Service (RDS) para garantir que as últimas atualizações de versões secundárias do sistema de gerenciamento de banco de dados relacional (RDBMS) estejam instaladas, o que pode incluir patches de segurança e correções de bugs.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	redshift-cluster-maintenancesettings-check	Essa regra garante que os clusters do Amazon Redshift tenham as configurações preferidas da organização. Especificamente, que eles tenham janelas de manutenção preferenciais e períodos automatizados de retenção de snapshots para o banco de dados. Essa regra exige que você defina allowVersionUpgrade o. O padrão é true. Também permite definir opcionalmente o preferredMaintenanceWindow (o padrão é sat: 16:00 -sat: 16:30) e o automatedSnapshotRetentionPeríodo (o padrão é 1). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.3	Vulnerability Management	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Plano de gerenciamento de crises cibernéticas	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Plano de gerenciamento de crises cibernéticas	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Plano de gerenciamento de crises cibernéticas	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Plano de gerenciamento de crises cibernéticas	ec2-managedinstance-association-compliance-status-check	Use o AWS Systems Manager Associations para ajudar no inventário de plataformas e aplicativos de software em uma organização. AWS O Systems Manager atribui um estado de configuração às suas instâncias gerenciadas e permite que você defina linhas de base dos níveis de patch do sistema operacional, instalações de software, configurações de aplicativos e outros detalhes sobre seu ambiente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.5	Plano de gerenciamento de crises cibernéticas	ec2-managedinstance-patch-compliance-status-check	Habilite essa regra para ajudar na identificação e documentação das vulnerabilidades do Amazon Elastic Compute Cloud (Amazon EC2). A regra verifica se as instâncias do Amazon EC2 estão em conformidade com patches no AWS Systems Manager, conforme exigido pelas políticas e procedimentos da sua organização.
3.9	Avaliação de risco de TI	annual-risk-assessment-performed (verificação do processo)	Faça uma avaliação anual de risco em sua organização. As avaliações de risco podem ajudar a determinar a probabilidade e o impacto dos riscos e/ou vulnerabilidades identificados que afetam uma organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
3.12	Treinamento	security-awareness-program-exists (verificação do processo)	Estabeleça e mantenha um programa de conscientização sobre segurança para sua organização. Os programas de conscientização sobre segurança instruem os funcionários sobre como proteger sua organização contra várias violações ou incidentes de segurança.
4.4(g)	Análise de fraudes: análise de transações suspeitas, peculato, roubo ou suspeita de lavagem de dinheiro, apropriação indébita de ativos, manipulação de registros financeiros, etc. A exigência regulatória de denunciar fraudes ao RBI deve ser orientada pelo sistema.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	clb-multiple-az	O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibilidade diferentes para garantir que sua função esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibilidade funciona em sua própria infraestrutura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestrutura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	s3-bucket-default-lock-enabled	Habilite o bloqueio do bucket do Amazon Simple Storage Service (Amazon S3) por padrão. Como pode haver dados confidenciais em repouso nos buckets do S3, aplique bloqueios de objetos em repouso para ajudar a protegê-los.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implementados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-Site para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativas de conexão ou envia solicitações para testar a integridade de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver respondendo, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
4.4(h)	Análise de capacidad e e performance de sistemas de segurança de TI.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.
4.4(h)	Análise de capacidad e e performance de sistemas de segurança de TI.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	lambda-dlq-check	Habilite essa regra para ajudar a notificar a equipe adequada por meio do Amazon Simple Queue Service (Amazon SQS) ou do Amazon Simple Notification Service (Amazon SNS) quando uma função falhar.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	beanstalk-enhanced-health-reporting-enabled	AWS Os relatórios de saúde aprimorados do Elastic Beanstalk permitem uma resposta mais rápida às mudanças na integridade da infraestrutura subjacente. Essas alterações podem resultar na falta de disponibilidade do aplicativo. Os relatórios de integrida de aprimorados do Elastic Beanstalk fornecem um descritor de status para avaliar a gravidade dos problemas identificados e descobrir possíveis causas a serem investigadas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	ebs-optimized-instance	Uma instância otimizada no Amazon Elastic Block Store (Amazon EBS) fornece capacidade adicional e dedicada para operações de E/S do Amazon EBS. Essa otimização proporciona o melhor desempenho para os volumes do EBS, minimizando a contenção entre a E/S do Amazon EBS e outros tráfegos da instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(h)	Análise de capacidade e performance de sistemas de segurança de TI.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(i)	Relatórios de incidentes, seu impacto e medidas tomadas para a não recorrência de tais eventos no futuro.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
4.4(i)	Relatórios de incidentes, seu impacto e medidas tomadas para a não recorrência de tais eventos no futuro.	guardduty-non-archived-findings	GuardDuty A Amazon ajuda você a entender o impacto de um incidente classificando as descobertas por gravidade: baixa, média e alta. É possível usar essas classificações para determinar estratégias e prioridades de correção. Essa regra permite que você defina opcionalmente daysLowSev (Config Default: 30), daysMediumSev (Config Default: 7) e daysHighSev (Config Default: 1) para descobertas não arquivadas, conforme exigido pelas políticas da sua organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	aurora-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Aurora façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	cmk-backing-key-rotation-enabled	Ative a rotação de chaves para garantir que as chaves sejam giradas após atingirem o final do período criptográfico.
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específicos para atender aos requisitos de resiliência.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	ec2-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus recursos do Amazon Elastic Compute Cloud (Amazon EC2) façam parte de um plano de Backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessári os para seus sistemas comerciais e datacenters essenciai s.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	fsx-resources-protected-by-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos Amazon FSx façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodicamente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
6.3	Os NBFCs devem considerar a necessidade de criar os locais de backup necessários para seus sistemas comerciais e datacenters essenciais.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	dynamodb-autoscaling-enabled	O Amazon DynamoDB auto scaling usa o serviço Application AWS Auto Scaling para ajustar a capacidade de transferência provisionada que responde automaticamente aos padrões reais de tráfego. Isso permite que uma tabela ou um índice secundário global aumente a capacidade provisionada de leitura e gravação para processar aumentos repentinos no tráfego, sem controle de utilização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	elb-cross-zone-load-balancing-enabled	Habilite o balanceamento de carga entre zonas para os Elastic Load Balancers (ELBs) para ajudar a manter a capacidade e a disponibilidade adequadas. O balanceamento de carga entre zonas reduz a necessidade de manter números equivalentes de instâncias em cada zona de disponibilidade habilitada. Também melhora a capacidade da aplicação de lidar com a perda de uma ou mais instâncias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	elb-deletion-protection-enabled	Essa regra garante que o Elastic Load Balancing tenha a proteção contra exclusão habilitada. Use esse recurso para evitar que o balanceador de carga seja excluído de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	clb-multiple-az	O Elastic Load Balancing (ELB) distribui automaticamente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibilidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	elbv2-multiple-az	O Elastic Load Balancing (ELB) distribui automatic amente o tráfego de entrada entre vários destinos, como instâncias do EC2, contêineres e endereços IP, em uma ou mais zonas de disponibilidade. Para garantir alta disponibilidade, o ELB deve ter instâncias registradas de várias zonas de disponibi lidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	lambda-vpc-multi-az-check	Se sua função AWS Lambda estiver configurada para se conectar a uma nuvem privada virtual (VPC) em sua conta, implante a função AWS Lambda em pelo menos duas zonas de disponibi lidade diferentes para garantir que sua função esteja disponível para processar eventos em caso de interrupção do serviço em uma única zona.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	rds-instance-deletion-protection-enabled	Habilite a proteção contra exclusão das instâncias do Amazon Relational Database Service (Amazon RDS). Use a proteção contra exclusão para evitar que as instâncias do Amazon RDS sejam excluídas de forma acidental ou mal-intencionada, o que pode levar à perda de disponibilidade das aplicações.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	rds-multi-az-support	O suporte multi-AZ no Amazon Relational Database Service (Amazon RDS) oferece maior disponibilidade e durabilidade para instâncias de banco de dados. Ao provisionar uma instância de banco de dados multi-AZ, o Amazon RDS cria automaticamente uma instância de banco de dados primária e replica de forma síncrona os dados em uma instância em modo de espera em outra zona de disponibilidade. Cada zona de disponibi lidade funciona em sua própria infraestr utura independente e fisicamente distinta, além de ser projetada para ser altamente confiável. No caso de falha na infraestr utura, o Amazon RDS executa um

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			failover automático no modo de espera para que você possa retomar as operações do banco de dados assim que o failover for concluído.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	vpc-vpn-2-tunnels-up	Túneis redundantes do VPN Site-to-Site podem ser implement ados para atender aos requisitos de resiliência. Dois túneis são usados para ajudar a garantir a conectividade caso uma das conexões do VPN Site-to-Site fique indisponível. A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, use um segundo gateway do cliente e configure uma segunda conexão do VPN Site-to-S ite para o Amazon Virtual Private Cloud (Amazon VPC) e para o gateway privado virtual.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	autoscaling-group-elb-healthcheck-required	As verificações de integridade do Elastic Load Balancer (ELB) para grupos do Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling contribuem para a manutenção de níveis adequados de capacidade e disponibilidade. O balanceador de carga periodicamente envia pings, faz tentativa s de conexão ou envia solicitações para testar a integrida de de instâncias do Amazon EC2 em um grupo de ajuste de escala automático. Se uma instância não estiver responden do, o tráfego será enviado para uma nova instância do Amazon EC2.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	dynamodb-throughput-limit-check	Habilite essa regra para garantir que a capacidade de throughput provisionada seja verificada em suas tabelas do Amazon DynamoDB. Essa é a quantidade de atividades de leitura e gravação que cada tabela pode comportar. O DynamoDB usa essas informações para reservar recursos suficientes do sistema para atender aos seus requisitos de throughput. Essa regra gera um alerta quando o throughput se aproxima do limite máximo da conta de um cliente. Essa regra permite que você defina opcionalmente os parâmetros AccountRCUThresholdPercentage (Config Default: 80) e AccountWCUThresholdPercentage (Config Default:

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			80). Os valores reais devem refletir as políticas da organizaç ão.
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoram ento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoram ento com um período de 1 minuto para a instância.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs malicioso s e aprendizado de máquina para identificar atividade s inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	lambda-concurrency-check	Essa regra garante que os limites altos e baixos de simultane idade de uma função do Lambda sejam estabelecidos. Isso pode ajudar a definir o número de solicitaç ões que a função atende em determina do momento.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	rds-enhanced-monitoring-enabled	Habilite o Amazon Relational Database Service (Amazon RDS) para ajudar a monitorar a disponibilidade do Amazon RDS. Isso fornece visibilidade detalhada da integridade das instâncias de banco de dados do Amazon RDS. Quando o armazenamento do Amazon RDS está usando mais de um dispositivo físico subjacente, o monitoramento avançado coleta os dados de cada dispositivo. Além disso, quando a instância do banco de dados do Amazon RDS está sendo executada em uma implantação multi-AZ, os dados de cada dispositivo no host secundário são coletados, bem como as respectivas das métricas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.1	Os sistemas de TI devem ser ampliados progressivamente à medida que o tamanho e a complexidade das operações da NBFC aumentam.	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são Amazon Security Hub, Amazon Inspector, Amazon Macie AWS , Identity and Access Management (IAM) Access Analyzer, Firewall AWS Manager e soluções de parceiros. AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-bucket-policy-grantee-check	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check. Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principais de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	dms-replication-not-public	Gerencie o acesso à AWS nuvem garantindo que as instâncias de replicação do DMS não possam ser acessadas publicamente. As instâncias de replicação do DMS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ebs-snapshot-public-restorable-check	Gerencie o acesso à AWS nuvem garantindo que os instantâneos do EBS não sejam restauráveis publicamente. Os snapshots de volume do EBS podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	elasticsearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service (OpenSearch Service) estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio OpenSearch de serviço em uma Amazon VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	emr-master-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que os nós principais do cluster Amazon EMR não possam ser acessados publicamente. Os nós principais do cluster do Amazon EMR podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantind o que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizad o aos recursos do Amazon VPC.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicação segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessida de de um gateway da Internet, dispositi vo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadamente o acesso, as funções do AWS Lambda devem

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			ser atribuídas a uma VPC.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	rds-instance-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	rds-snapshots-public-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as instâncias do Amazon Relationa l Database Service (Amazon RDS) não sejam públicas. As instâncias de banco de dados do Amazon RDS podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	redshift-cluster-public-access-check	Gerencie o acesso aos recursos na AWS nuvem garantindo que os clusters do Amazon Redshift não sejam públicos. Os clusters do Amazon Redshift podem conter informaçõ es confidenciais e princípios, e o controle de acesso é necessário para essas contas.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalm ente os parâmetros blockedPort1-block edPort5 (Padrões de configuração: 20.21.3389.3306.43 33). Os valores reais devem refletir as políticas da organizaç ão.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	sagemaker-notebook-no-direct-internet-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que os SageMaker notebooks da Amazon não permitam acesso direto à Internet. Ao impedir o acesso direto à internet, você impede que dados confidenciais sejam acessados por usuários não autorizados.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciam ento do acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibi lidade, a integridade e a confidencialidade dos sistemas. Ao restringir o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especificado pela política organizacional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternância da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	emr-kerberos-enabled	Ao habilitar o Kerberos para clusters do Amazon EMR, é possível gerenciar e incorporar as permissões e autorizações de acesso com os princípios de privilégio mínimo e separação de deveres. No Kerberos, os serviços e os usuários que precisam se autenticar são conhecidos como entidades principais. As entidades principais existem em um realm Kerberos. No realm, um servidor Kerberos é conhecido como o centro de distribuição de chaves (KDC). Ele fornece um meio para as entidades principais se autenticarem. A autenticação do KDC é feita com a emissão de tíquetes. O KDC mantém um banco de dados das entidades principais no realm,

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			as senhas e outras informações administrativas sobre cada entidade principal.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.l	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	autoscaling-launch-config-public-ip-disabled	Se você configurar suas interfaces de rede com um endereço IP público, os recursos associados a elas poderão ser acessados pela internet. Os recursos do EC2 não devem permitir acesso público, pois isso permite acesso não intencional a aplicações ou servidores.
8.l	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ecs-task-definition-nonroot-user	Para ajudar na implementação do princípio de privilégio mínimo, garanta que um usuário não raiz seja designado para acessar suas definições de tarefas do Amazon Elastic Container Service (Amazon ECS).

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	efs-access-point-enforce-root-directory	A aplicação de um diretório raiz para um ponto de acesso do Amazon Elastic File System (Amazon EFS) ajuda a restringir o acesso aos dados, garantindo que os usuários do ponto de acesso só possam acessar arquivos do subdiretório especificado.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	efs-access-point-enforce-user-identity	Para ajudar na implementação do princípio de privilégio mínimo, habilite a fiscalização do usuário para o Amazon Elastic File System (Amazon EFS). Quando habilitada, o Amazon EFS substitui os IDs de usuário e grupo do cliente NFS pela identidade configurada no ponto de acesso para todas as operações do sistema de arquivos e concede acesso somente a essa identidade de usuário imposta.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Management (IAM). Em vez de ACLs, é uma prática recomendada usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo o que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencional aos seus documentos SSM. Um documento do SSM público pode expor informações sobre sua conta, recursos e processos internos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	subnet-auto-assign-public-ip-disabled	Gerencie o acesso à AWS nuvem garantindo que as sub-redes da Amazon Virtual Private Cloud (VPC) não recebam automaticamente um endereço IP público. As instância s do Amazon Elastic Compute Cloud (EC2) que são executada s em sub-redes com esse atributo habilitad o têm um endereço IP público atribuído à sua interface de rede primária.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verificando se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas compromet idas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	opensearch-in-vpc-only	Gerencie o acesso à AWS nuvem garantindo que os domínios do Amazon OpenSearch Service estejam dentro de uma Amazon Virtual Private Cloud (Amazon VPC). Um domínio do Amazon OpenSearch Service dentro de um Amazon VPC permite a comunicação segura entre o Amazon OpenSearch Service e outros serviços dentro do Amazon VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.I	Aspectos básicos de segurança, como controles de acesso físico/lógico e política de senha bem definida.	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-group-has-users-check	AWS O Identity and Access Managemen t (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantind o que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associada s ou na função de trabalho é uma forma de incorporar o privilégio mínimo.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas. As políticas gerenciadas permitem a reutiliza ção, o versionam ento, a reversão e a delegação do gerenciamento de permissões.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-password-policy	As identidades e as credenciais são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLowercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			o), RequireNumbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePrevention (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswordAge (valor das melhores práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-policy-no-statements-with-admin-access	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, impedindo que as políticas contenham “Efeito”: “Permitir” com “Ação”: “*” sobre “Recurso” : “*”. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Managemen t (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuiçã o de privilégios por grupo ou perfil ajuda a reduzir a oportunid ade de uma identidad e receber ou reter privilégios excessivos.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8.II	Uma função de usuário bem definida.	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsageIdade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. III	Um conceito Maker-Checker para reduzir o risco de erro e uso indevido e garantir a confiabilidade dos dados/informações.	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionam ento ajuda você a se recuperar facilment e de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	db-instance-backup-enabled	O recurso de backup do Amazon RDS cria backups dos bancos de dados e logs de transações. O Amazon RDS cria automaticamente um snapshot do volume de armazenamento da instância de banco de dados, fazendo backup de toda a instância de banco de dados. O sistema permite que você defina períodos de retenção específic os para atender aos requisitos de resiliênc ia.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	dynamodb-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas tabelas do Amazon DynamoDB façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	dynamodb-pitr-enabled	Habilite essa regra para verificar se o backup das informações foi realizado. Ele também mantém os backups, garantindo que a point-in-time recuperação seja habilitada no Amazon DynamoDB. A recuperação mantém backups contínuos da tabela nos últimos 35 dias.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplific a o gerenciamento de backup e permite que você atenda aos requisitos comerciai s e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	elasticache-redis-cluster-automatic-backup-check	Quando os backups automáticos estão habilitados, a Amazon ElastiCache cria um backup do cluster diariamente. O backup pode ser retido por vários dias, conforme especific ado pela organização. Os backups automátic os podem ajudar a proteger contra a perda de dados. Em caso de falha, é possível criar um cluster e restaurar os dados usando o backup mais recente.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	rds-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que suas instâncias do Amazon Relational Database Service (Amazon RDS) façam parte de um AWS plano de backup. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	s3-bucket-replication-enabled	A Replicação entre regiões (CRR) do Amazon Simple Storage Service (Amazon S3) é compatível com a manutenção de capacidade e disponibilidade adequadas. A CRR permite a cópia automática e assíncrona de objetos nos buckets do Amazon S3 para ajudar a garantir a manutenção da disponibilidade de dados.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	redshift-backup-enabled	Para ajudar nos processos de backup de dados, os clusters do Amazon Redshift devem ter snapshots automatizados. Quando snapshots automatizados são habilitados para um cluster, o Redshift tira snapshots desse cluster periodica mente. Por padrão, o Redshift tira um instantâneo a cada oito horas ou a cada 5 GB para cada nó de alteração de dados, ou o que ocorrer primeiro.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	backup-plan-min-frequency-and-min-retention-check	Para ajudar nos processos de backup de dados, certifique-se de que seu plano de AWS backup esteja definido para uma frequência e retenção mínimas. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina os requiredFrequencyValue parâmetros (Config default: 1), (requiredRetentionDays Config default: 35) e (requiredFrequencyUnit Config default: days). O valor real deve refletir

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
			os requisitos da organização.
8. IX	Organização de backup de dados com testes periódicos.	backup-recovery-point-manual-deletion-disabled	Certifique-se de que seus pontos AWS de recuperação de Backup tenham uma política baseada em recursos anexada que impeça a exclusão de pontos de recuperação. Usar uma política baseada em recursos para impedir a exclusão de pontos de recuperação pode ajudar a evitar a exclusão acidental ou intencional.

ID de controle	Descrição do controle	AWS Regra de configuração	Orientação
8. IX	Organização de backup de dados com testes periódicos.	backup-recovery-point-minimum-retention-check	Para ajudar nos processos de backup de dados, garanta que seus pontos de recuperação de AWS backup tenham um período mínimo de retenção definido. AWS O Backup é um serviço de backup totalmente gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups. Essa regra permite que você defina o parâmetro requiredRetentionDays (configuração padrão: 35). O valor real deve refletir os requisitos da organização.

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o RBI MD-ITF.

Práticas recomendadas operacionais para serviços de segurança, identidade e conformidade

Esse pacote de conformidade contém AWS Config regras baseadas em serviços de segurança, identidade e conformidade. Para obter mais informações, consulte Segurança, identidade e conformidade em AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de segurança, identidade e conformidade.

Práticas recomendadas operacionais para tecnologia sem servidor

Esse pacote de conformidade contém AWS Config regras baseadas em soluções sem servidor. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para sistemas sem servidor.

Práticas recomendadas operacionais para serviços de armazenamento

Esse pacote de conformidade contém AWS Config regras baseadas nos Serviços de Armazenamento. Para obter mais informações, consulte Cloud Storage ativado AWS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas operacionais para serviços de armazenamento.

Práticas recomendadas operacionais para SWIFT CSP

Os pacotes de conformidade fornecem uma estrutura de conformidade de uso geral projetada para permitir que você crie verificações de governança de segurança, operação ou otimização de custos usando regras e ações de remediação gerenciadas ou personalizadas. AWS Config AWS Config Os pacotes de conformidade, como os modelos de amostra, não foram projetados para garantir totalmente a conformidade com um padrão específico de governança ou conformidade. Você é responsável por avaliar se o seu uso dos serviços atende aos requisitos legais e regulamentares aplicáveis.

Veja a seguir um exemplo de mapeamento entre o Programa de Segurança do Cliente (CSP) da SWIFT e as regras gerenciadas do AWS Config. Cada AWS Config regra se aplica a um AWS recurso específico e está relacionada a um ou mais controles SWIFT CSP. Um controle CSP SWIFT pode estar relacionado a várias AWS Config regras. Consulte a tabela abaixo para conferir mais detalhes e orientações relacionados a esses mapeamentos.

ID de controle	AWS Regra de configuração	Orientação
1.1	ec2-instance-managed-by-systems-manager	É possível fazer um inventário das plataformas de software e aplicativos dentro da organização gerenciando as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com o Systems Manager. AWS Use o AWS Systems Manager para fornecer configurações detalhadas do sistema, níveis de patch do sistema operacional, nome e tipo de serviços, instalações de software, nome do aplicativo, editor e versão, além de outros detalhes sobre seu ambiente.
1.1	ec2-instance-no-public-ip	Gerencie o acesso à AWS nuvem garantindo que as

ID de controle	AWS Regra de configuração	Orientação
		instâncias do Amazon Elastic Compute Cloud (Amazon EC2) não possam ser acessadas publicamente. As instâncias do Amazon EC2 podem conter informações confidenciais, e o controle de acesso é necessário para essas contas.
1.1	ec2-no-amazon-key-pair	Essa regra verifica se as instâncias em execução do Amazon Elastic Compute Cloud (Amazon EC2) são iniciadas usando pares de chaves da Amazon. Isso pode ajudar a reduzir o risco de credenciais comprometidas. As instâncias do Amazon EC2 sem pares de chaves ainda podem ser acessadas usando o Session Manager ou a conexão SSH baseada em navegador por meio do console. AWS

ID de controle	AWS Regra de configuração	Orientação
1.1	ec2-instances-in-vpc	Implemente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) em um Amazon Virtual Private Cloud (Amazon VPC) para permitir a comunicação segura entre uma instância e outros serviços no Amazon VPC, sem exigir um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolament o lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Atribua instâncias do Amazon EC2 a um Amazon VPC para gerenciar adequadamente o acesso.

ID de controle	AWS Regra de configuração	Orientação
1.1	vpc-default-security-group-closed	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar no gerenciamento do acesso à rede fornecend o filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Restringir todo o tráfego no grupo de segurança padrão ajuda a restringir o acesso remoto aos seus AWS recursos.
1.1	vpc-network-acl-unused-check	Essa regra garante que as listas de controle de acesso à rede do Amazon Virtual Private Cloud (VPC) estejam em uso. O monitoramento de listas de controle de acesso à rede não utilizadas pode ajudar a manter a precisão do inventário e do gerenciamento em seu ambiente.

ID de controle	AWS Regra de configuração	Orientação
1.1	vpc-sg-open-only-to-authorized-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integrida de e a confidencialidade dos sistemas. Ao restringi r o acesso a recursos em um grupo de segurança da internet (0.0.0.0/0), o acesso remoto pode ser controlado para sistemas internos.

ID de controle	AWS Regra de configuração	Orientação
1.2	iam-customer-policy-blocked-kms-actions	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de tarefas com permissões e autorizaç ões de acesso, impedindo que as políticas contenham ações bloqueadas em AWS todas as chaves do Key Management Service. Ter mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres. Essa regra permite que você defina o blockedActionsPatt erns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1.2	iam-group-has-users-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a incorporar os princípios de privilégio mínimo e separação de deveres com permissões e autorizações de acesso, garantindo que os grupos do IAM tenham pelo menos um usuário. Colocar usuários em grupos com base nas permissões associadas ou na função de trabalho é uma forma de incorporar o privilégi o mínimo.

ID de controle	AWS Regra de configuração	Orientação
1.2	iam-inline-policy-blocked-kms-actions	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para permitir ações bloqueadas em AWS todas as chaves do Key Management Service. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciam ento de permissões. Essa regra permite que você defina o blockedActionsPatterns parâmetro. (Valor AWS básico das melhores práticas de segurança: kms:Decrypt, kms: From). ReEncrypt Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1.2	iam-no-inline-policy-check	Certifique-se de que um usuário, uma função do IAM ou um grupo do IAM do AWS Identity and Access Management (IAM) não tenha uma política embutida para controlar o acesso a sistemas e ativos. AWS recomenda usar políticas gerenciadas em vez de políticas embutidas . As políticas gerenciadas permitem a reutilização, o versionamento, a reversão e a delegação do gerenciamento de permissões.
1.2	iam-user-no-policies-check	Essa regra garante que as políticas de AWS Identity and Access Management (IAM) sejam anexadas somente a grupos ou funções para controlar o acesso a sistemas e ativos. A atribuição de privilégios por grupo ou perfil ajuda a reduzir a oportunidade de uma identidade receber ou reter privilégios excessivos.

ID de controle	AWS Regra de configuração	Orientação
1.2	restricted-ssh	Os grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2) podem ajudar a gerenciar o acesso à rede fornecendo filtragem monitorada do tráfego de entrada e saída da rede aos recursos. AWS Não permitir o tráfego de entrada (ou remoto) de 0.0.0.0/0 para a porta 22 nos recursos ajuda a restringir o acesso remoto.
1.2	nacl-no-unrestricted-ssh-rdp	As portas de administração do servidor remoto em suas listas de controle de acesso à rede (ACL da rede), como a porta 22 (SSH) e a porta 3389 (RDP), não devem ser acessíveis ao público, pois isso pode permitir acesso não intencional a recursos na VPC.

ID de controle	AWS Regra de configuração	Orientação
1.2	s3-bucket-acl-prohibited	Essa regra verifica se as listas de controle de acesso (ACLs) são usadas para controle de acesso nos buckets do Amazon S3. As ACLs são mecanismos legados de controle de acesso para buckets do Amazon S3 AWS anteriores ao Identity and Access Managemen t (IAM). Em vez de ACLs, é uma prática recomenda da usar políticas do IAM ou políticas de bucket do S3 para gerenciar mais facilmente o acesso aos buckets do S3.

ID de controle	AWS Regra de configuração	Orientação
1.2	s3-bucket-logging-enabled	O registro em log de acesso ao servidor do Amazon Simple Storage Service (Amazon S3) fornece um método para monitorar a rede em busca de possíveis eventos de segurança cibernética. Os eventos são monitorados pela captura de registros detalhado s das solicitações que são feitas a um bucket do Amazon S3. Cada registro de log de acesso fornece detalhes sobre uma única solicitaç ão de acesso. Os detalhes incluem solicitante, nome do bucket, horário da solicitação, ação da solicitação, status da resposta e um código de erro, se relevante.
1.2	s3-bucket-policy-grantee-ch eck	Gerencie o acesso à AWS nuvem ativando s3_ bucket_policy_grantee_check . Essa regra verifica se o acesso concedido pelo bucket do Amazon S3 é restrito por qualquer um dos AWS principais, usuários federados, entidades principai s de serviços, endereços IP ou IDs da Amazon Virtual Private Cloud (Amazon VPC) fornecidos por você.

ID de controle	AWS Regra de configuração	Orientação
1.2	sns-topic-message-delivery-notification-enabled	Para ajudar com os requisitos de registro em log em seu ambiente, garanta a habilitação das notificações de status de entrega para os tópicos do Amazon Simple Notification Service (Amazon SNS). O registro em log do status de entrega da mensagem ajuda a fornecer uma melhor visão operacional, como a seguinte: saber se uma mensagem foi entregue ao endpoint do Amazon SNS, identificar a resposta enviada do endpoint do Amazon SNS para o Amazon SNS e determinar o tempo de permanência da mensagem (o tempo entre o timestamp da publicação e pouco antes da entrega para um endpoint do Amazon SNS).

ID de controle	AWS Regra de configuração	Orientação
1.4	internet-gateway-authorized-vpc-only	Gerencie o acesso aos recursos na AWS nuvem garantindo que os gateways de internet estejam conectados somente à Amazon Virtual Private Cloud autorizada (Amazon VPC). Os gateways da Internet permitem acesso bidirecional entre a internet e o Amazon VPC, o que pode ocasionar acesso não autorizado aos recursos do Amazon VPC.
1.4	restricted-common-ports	Gerencie o acesso aos recursos na AWS nuvem garantindo que as portas comuns sejam restritas nos grupos de segurança do Amazon Elastic Compute Cloud (Amazon EC2). Não restringir o acesso às portas a fontes confiáveis pode permitir ataques contra a disponibilidade, a integridade e a confidencialidade dos sistemas. Essa regra permite que você defina opcionalmente os parâmetros blockedPort1-blockedPort5 (Padrões de configuração: 20.21.3389.3306.4333). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1.4	lambda-function-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que as funções do AWS Lambda não possam ser acessadas publicamente. O acesso público pode causar degradação da disponibilidade de recursos.
1.4	s3-account-level-public-access-blocks-periodic	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público. Essa regra permite que você defina opcionalmente ignorePublicAcls (Config Default: True), blockPublicPolicy (Config Default: True), blockPublicAcls (Config Default: True) e restrictPublicBuckets parâmetros (Config Default: True). Os valores reais devem refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
1.4	s3-bucket-level-public-access-prohibited	Gerencie o acesso aos recursos na AWS nuvem garantindo que os buckets do Amazon Simple Storage Service (Amazon S3) não possam ser acessados publicamente. Essa regra ajuda a manter os dados confidenciais protegidos de usuários remotos não autorizados, impedindo o acesso público no nível do bucket.
1.4	s3-bucket-public-read-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.
1.4	s3-bucket-public-write-prohibited	Gerencie o acesso aos recursos na AWS nuvem permitindo que somente usuários, processos e dispositivos autorizados acessem os buckets do Amazon Simple Storage Service (Amazon S3). O gerenciamento do acesso deve ser consistente com a classificação dos dados.

ID de controle	AWS Regra de configuração	Orientação
1.4	ssm-document-not-public	Certifique-se AWS de que os documentos do Systems Manager (SSM) não sejam públicos, pois isso pode permitir acesso não intencion al aos seus documentos SSM. Um documento do SSM público pode expor informaçõ es sobre sua conta, recursos e processos internos.
2.3	ec2-imdsv2-check	Habilite o método serviço de metadados de instância versão 2 (IMDSv2) para ajudar a proteger o acesso e o controle dos metadados da instância do Amazon Elastic Compute Cloud (Amazon EC2). O método IMDSv2 usa controles baseados em sessão. Com o IMDSv2, os controles podem ser implementados para restringir alterações nos metadados da instância.

ID de controle	AWS Regra de configuração	Orientação
2.3	ec2-instance-multiple-eni-check	Essa regra verifica se suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) têm vários ENIs. Ter vários ENIs pode causar instâncias com hospedagem dupla, ou seja, instâncias com várias sub-redes. Isso pode aumentar a complexidade da segurança da rede e introduzir caminhos e acessos de rede não intencionais.
2.3	ec2-token-hop-limit-check	A resposta HTTP PUT do serviço de metadados de instância (IMDS) deve ser restrita à instância do Amazon Elastic Compute Cloud (Amazon EC2). Com o IMDSv2, a resposta PUT que contém o token secreto por padrão não pode sair da instância, porque o limite de salto de resposta de metadados está definido como 1 (padrão do Config). Se esse valor for maior que 1, o token poderá sair da instância do EC2.

ID de controle	AWS Regra de configuração	Orientação
2.3	ec2-volume-inuse-check	Essa regra garante que os volumes do Amazon Elastic Block Store que estão anexados às instâncias do Amazon Elastic Compute Cloud (Amazon EC2) sejam marcados para exclusão quando uma instância é encerrada. Se um volume do Amazon EBS não for excluído quando a instância à qual ele está anexado for encerrada, ele poderá violar o conceito de funcionalidade mínima.
2.3	account-part-of-organizations	O gerenciamento centralizado de Contas da AWS dentro das AWS Organizations ajuda a garantir que as contas estejam em conformidade. Usar uma governança não centralizada na conta pode gerar inconsist ências nas configurações da conta, o que pode expor recursos e dados confidenc iais.

ID de controle	AWS Regra de configuração	Orientação
2.3	lambda-inside-vpc	Implante funções AWS Lambda em uma Amazon Virtual Private Cloud (Amazon VPC) para uma comunicaç ão segura entre uma função e outros serviços dentro da Amazon VPC. Com essa configuração, não há necessidade de um gateway da Internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem no Amazon VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos. Para gerenciar adequadam ente o acesso, as funções do AWS Lambda devem ser atribuídas a uma VPC.

ID de controle	AWS Regra de configuração	Orientação
2.3	kms-cmk-not-scheduled-for-deletion	Para ajudar a proteger os dados em repouso, certifique-se de que as chaves mestras do cliente (CMKs) necessárias não estejam programadas para exclusão no AWS Key Management Service (AWS KMS). Como às vezes a exclusão da chave é necessária, essa regra pode ajudar na verificação de todas as chaves programadas para exclusão, caso alguma delas sido programada de maneira não intencional.
2.3	s3-bucket-versioning-enabled	O versionamento do bucket do Amazon Simple Storage Service (Amazon S3) ajuda a manter diversas variantes de um objeto no mesmo bucket do Amazon S3. Use o versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket do Amazon S3. O versionamento ajuda você a se recuperar facilmente de ações não intencionais de usuários e de falhas da aplicação.

ID de controle	AWS Regra de configuração	Orientação
2.3	secretsmanager-secret-unused	Se existirem credenciais não utilizadas no AWS Secrets Manager, você deve desativar e/ou remover as credencia is, pois isso pode violar o princípio do menor privilégi o. Essa regra permite que você defina um valor para unusedForDays (Config Default: 90). O valor real deve refletir as políticas da organização.
2.5A	ebs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus volumes do Amazon Elastic Block Store (Amazon EBS) façam parte de um plano de backup. AWS AWS O Backup é um serviço de backup totalmente gerenciad o com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciam ento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2.5A	ec2-ebs-encryption-by-default	Para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS). Como pode haver dados confidenc iais em repouso nesses volumes, habilite a criptogra fia em repouso para ajudar a protegê-los.
2.5A	efs-encrypted-check	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Elastic File System (EFS).
2.5A	efs-in-backup-plan	Para ajudar nos processos de backup de dados, garanta que seus sistemas de arquivos do Amazon Elastic File System (Amazon EFS) façam parte de um plano de AWS backup. AWS O Backup é um serviço de backup totalment e gerenciado com uma solução de backup baseada em políticas. Essa solução simplifica o gerenciamento de backup e permite que você atenda aos requisitos comerciais e regulatórios de conformidade de backups.

ID de controle	AWS Regra de configuração	Orientação
2.5A	encrypted-volumes	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptografia para os volumes do Amazon Elastic Block Store (Amazon EBS).
2.5A	kinesis-stream-encrypted	Como pode haver dados confidenciais, e para ajudar a proteger os dados em repouso, habilite a criptogra fia para o Amazon Kinesis Streams.
2.5A	s3-bucket-server-side-encry ption-enabled	Para ajudar a proteger os dados em repouso, habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenc iais em repouso nos buckets do Amazon S3, habilite a criptografia para ajudar a protegê-los.
2.5A	s3-default-encryption-kms	Habilite a criptografia para os buckets do Amazon Simple Storage Service (Amazon S3). Como pode haver dados confidenciais em repouso em um bucket do Amazon S3, habilite a criptografia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
2.5A	sns-encrypted-kms	Para ajudar a proteger dados em repouso, garanta que seus tópicos do Amazon Simple Notification Service (Amazon SNS) exijam criptografia AWS usando o Key Management Service AWS (KMS). Como pode haver dados confidenciais em repouso em mensagens publicadas, habilite a criptogra fia em repouso para ajudar a protegê-los.

ID de controle	AWS Regra de configuração	Orientação
4.1	iam-password-policy	As identidades e as credencia is são emitidas, gerenciadas e verificadas com base em uma política organizacional de senhas do IAM. Eles atendem ou excedem os requisitos estabelecidos pelo NIST SP 800-63 e pelo padrão AWS Foundational Security Best Practices para a força da senha. Essa regra permite que você defina opcionalmente RequireUppercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireLo wercaseCharacters (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireSymbols (valor das melhores práticas de segurança AWS básicas: verdadeiro), RequireNu mbers (valor das melhores práticas de segurança AWS básicas: verdadeiro), MinimumPasswordLength (valor das melhores práticas de segurança AWS básicas: 14), PasswordReusePreve ntion (valor das melhores práticas de segurança AWS básicas: 24) e MaxPasswo rdAge (valor das melhores

ID de controle	AWS Regra de configuração	Orientação
		práticas de segurança AWS básica: 90) para seu IAM Política de senha. Os valores reais devem refletir as políticas da organização.
4.1	access-keys-rotated	As credenciais são auditadas para dispositivos, usuários e processos autorizados, garantindo que as chaves de acesso do IAM sejam alternadas conforme especific ado pela política organizac ional. Alterar as chaves de acesso regularmente é uma prática recomendada de segurança. Isso reduz o período em que uma chave de acesso permanece ativa e diminui o impacto nos negócios se as chaves forem comprometidas. Essa regra requer um valor de alternânc ia da chave de acesso (padrão do Config: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
4.2	iam-user-mfa-enabled	Ative essa regra para restringir o acesso aos recursos na AWS nuvem. Essa regra garante que a autenticação multifator (MFA) esteja habilitada para todos os usuários. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Reduza os incidentes de contas comprometidas exigindo que os usuários utilizem a MFA.
4.2	mfa-enabled-for-iam-console-access	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para todos os usuários do AWS Identity and Access Management (IAM) que tenham uma senha de console. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir que os usuários utilizem a MFA, você reduz os incidentes de contas comprometidas e impede que dados confidenciais sejam acessados por usuários não autorizados.

ID de controle	AWS Regra de configuração	Orientação
4.2	root-account-hardware-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA de hardware esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de comprometimento. Contas da AWS
4.2	root-account-mfa-enabled	Gerencie o acesso aos recursos na AWS nuvem garantindo que a MFA esteja habilitada para o usuário raiz. O usuário raiz é o mais privilegiado em uma Conta da AWS. A MFA adiciona uma camada extra de proteção, além das credenciais de login. Ao exigir MFA para o usuário raiz, você pode reduzir os incidentes de compromet imento. Contas da AWS

ID de controle	AWS Regra de configuração	Orientação
5.1	ec2-instance-profile-attached	Os perfis de instância do EC2 passam um perfil do IAM para uma instância do EC2. Anexar um perfil de instância às instâncias pode ajudar no gerenciamento de privilégio mínimo e permissões.
5.1	iam-policy-no-statements-with-full-access	Garanta que as ações do IAM estejam restritas somente às ações necessárias. Permitir que os usuários tenham mais privilégios do que o necessári o para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
5.1	iam-root-access-key-check	O acesso a sistemas e ativos pode ser controlado verifican do se o usuário raiz não tem chaves de acesso anexadas à sua função de AWS Identity and Access Management (IAM). Exclua as chaves de acesso raiz. Em vez disso, crie e use com base em funções Contas da AWS para ajudar a incorporar o princípio da menor funcionalidade.

ID de controle	AWS Regra de configuração	Orientação
5.1	iam-user-group-membership-check	AWS O Identity and Access Management (IAM) pode ajudá-lo a restringir permissões e autorizações de acesso, garantindo que os usuários sejam membros de pelo menos um grupo. Permitir que os usuários tenham mais privilégios do que o necessário para concluir uma tarefa pode violar o princípio de privilégio mínimo e separação de deveres.
5.1	iam-user-unused-credentials-check	AWS O Identity and Access Management (IAM) pode ajudá-lo com permissões e autorizações de acesso verificando senhas e chaves de acesso do IAM que não são usadas por um período de tempo especificado. Se essas credenciais não utilizadas forem identificadas, você deverá desabilitar e/ou removê-las, pois isso pode violar o princípio de privilégio mínimo. Essa regra exige que você defina um valor como maxCredentialUsage Idade (Config Default: 90). O valor real deve refletir as políticas da organização.

ID de controle	AWS Regra de configuração	Orientação
5.4	secretsmanager-rotation-enabled-check	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido.
5.4	secretsmanager-scheduled-rotation-success-check	Essa regra garante que AWS os segredos do Secrets Manager tenham sido rotacionados com sucesso de acordo com o cronograma de rotação. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo e, possivelmente, diminuir o impacto nos negócios se ele for comprometido.

ID de controle	AWS Regra de configuração	Orientação
5.4	secretsmanager-secret-periodic-rotation	Essa regra garante que AWS os segredos do Secrets Manager tenham a rotação periódica ativada. A alternância de segredos em uma programação regular pode reduzir o período em que um segredo fica ativo, além de diminuir o impacto nos negócios, se o segredo for comprometido. O valor padrão é 90 dias.
5.4	secretsmanager-using-cmk	Para ajudar a proteger os dados em repouso, garanta que a criptografia com o AWS Key Management Service (AWS KMS) esteja habilitada para AWS segredos do Secrets Manager. Como pode haver dados confidenciais em repouso nos segredos do Secrets Manager, habilite a criptografia em repouso para ajudar a protegê-los.
6.4	ec2-instance-detailed-monitoring-enabled	Habilite essa regra para ajudar a melhorar o monitoramento de instâncias do Amazon Elastic Compute Cloud (Amazon EC2) no console do Amazon EC2, que exibe gráficos de monitoramento com um período de 1 minuto para a instância.

ID de controle	AWS Regra de configuração	Orientação
6.4	cloudwatch-log-group-encrypted	Para ajudar a proteger dados confidenciais em repouso, garanta que a criptografia esteja habilitada para seus grupos de CloudWatch registros da Amazon.
6.4	cloud-trail-cloud-watch-logs-enabled	Use CloudWatch a Amazon para coletar e gerenciar centralmente a atividade de eventos de log. A inclusão de AWS CloudTrail dados fornece detalhes da atividade de chamadas de API em seu Conta da AWS.
6.4	cloudtrail-enabled	AWS CloudTrail pode ajudar na não repúdio gravando ações do AWS Management Console e chamadas de API. Você pode identificar os usuários e os Contas da AWS que chamaram um AWS serviço, o endereço IP de origem onde as chamadas foram geradas e os horários das chamadas. Os detalhes dos dados capturados são vistos no Conteúdo do AWS CloudTrail Registro.

ID de controle	AWS Regra de configuração	Orientação
6.4	cloud-trail-encryption-enabled	Como podem existir dados confidenciais e para ajudar a proteger os dados em repouso, garanta que a criptografia esteja habilitad a para suas AWS CloudTrail trilhas.
6.4	cloud-trail-log-file-validation-enabled	Utilize a validação do arquivo de AWS CloudTrail log para verificar a integridade dos CloudTrail registros. A validação do arquivo de log ajuda a determinar se um arquivo de log foi modificad o, excluído ou inalterado após a CloudTrail entrega. Esse recurso é criado usando algoritmos padrão do setor: SHA-256 para hashing e SHA-256 com RSA para assinaturas digitais. Isso torna computacionalmente inviável modificar, excluir ou CloudTrai l falsificar arquivos de log sem detecção.

ID de controle	AWS Regra de configuração	Orientação
6.4	ec2-stopped-instance	Habilite essa regra para ajudar na configuração básica das instâncias do Amazon Elastic Compute Cloud (Amazon EC2) verificando se essas instâncias do Amazon EC2 foram interrompidas por mais dias do que o permitido pelos padrões da organização.
6.4	vpc-flow-logs-enabled	Os logs de fluxo da VPC fornecem registros detalhado s de informações sobre o tráfego de IP de entrada e saída das interfaces de rede no Amazon Virtual Private Cloud (Amazon VPC). Por padrão, o registro de log de fluxo inclui valores para os diferentes componentes do fluxo de IP, incluindo a origem, o destino e o protocolo.
6.5A	guardduty-enabled-centralized	A Amazon GuardDuty pode ajudar a monitorar e detectar possíveis eventos de cibersegurança usando feeds de inteligência de ameaças. Isso inclui listas de IPs maliciosos e aprendizado de máquina para identificar atividades inesperadas, não autorizadas e maliciosas em seu ambiente de AWS nuvem.

ID de controle	AWS Regra de configuração	Orientação
6.5A	securityhub-enabled	AWS O Security Hub ajuda a monitorar pessoas, conexões, dispositivos e software não autorizados. AWS O Security Hub agrega, organiza e prioriza os alertas ou descobertas de segurança de vários serviços. AWS Alguns desses serviços são o Amazon Security Hub, o Amazon Inspector, o Amazon Macie AWS , o Identity and Access Management (IAM) Access Analyzer e o Firewall AWS Manager, além de soluções de parceiros. AWS

Modelo

O modelo está disponível em GitHub: Melhores práticas operacionais para o SWIFT CSP.

Práticas recomendadas de segurança do Amazon Elastic Container Service (Amazon ECS)

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon ECS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon ECS.

Práticas recomendadas de segurança do Amazon Elastic File System (Amazon EFS)

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon EFS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon EFS.

Práticas recomendadas de segurança do Amazon Elastic Kubernetes Service (Amazon EKS)

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon EKS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon EKS.

Melhores práticas de segurança para a Amazon CloudFront

Este pacote de conformidade contém AWS Config regras baseadas na Amazon. CloudFront Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para a Amazon CloudFront.

Melhores práticas de segurança para o Amazon OpenSearch Service

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon OpenSearch Service. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para Amazon OpenSearch Service.

Práticas recomendadas de segurança para o Amazon Redshift

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon Redshift. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon Redshift.

Práticas recomendadas de segurança do Amazon Relational Database Service (Amazon RDS)

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon RDS. Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon RDS.

Práticas recomendadas de segurança do AWS Auto Scaling

Este pacote de conformidade contém AWS Config regras baseadas em. AWS Auto Scaling Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS Auto Scaling.

Práticas recomendadas de segurança do AWS CloudTrail

Este pacote de conformidade contém AWS Config regras baseadas em. AWS CloudTrail Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS CloudTrail.

Práticas recomendadas de segurança do AWS CodeBuild

Este pacote de conformidade contém AWS Config regras baseadas em. AWS CodeBuild Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS CodeBuild.

Práticas recomendadas de segurança para o Amazon ECR

Esse pacote de conformidade contém AWS Config regras baseadas no Amazon Elastic Container Registry (Amazon ECR). Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para o Amazon ECR.

Práticas recomendadas de segurança do AWS Lambda

Este pacote de conformidade contém AWS Config regras baseadas em. AWS Lambda Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS Lambda.

Práticas recomendadas de segurança do AWS Network Firewall

Este pacote de conformidade contém AWS Config regras baseadas em. AWS Network Firewall Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS Network Firewall.

Melhores práticas de segurança para a Amazon SageMaker

Este pacote de conformidade contém AWS Config regras baseadas na Amazon. SageMaker Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para a Amazon SageMaker.

Práticas recomendadas de segurança do AWS Secrets Manager

Este pacote de conformidade contém AWS Config regras baseadas em. AWS Secrets Manager Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS Secrets Manager.

Práticas recomendadas de segurança do AWS WAF

Este pacote de conformidade contém AWS Config regras baseadas em. AWS WAF Para obter uma lista de todas as regras gerenciadas suportadas pelo AWS Config, consulte Lista de regras AWS Config gerenciadas.

Consulte a `Parameters` seção no modelo a seguir para obter os nomes e as descrições dos parâmetros necessários.

O modelo está disponível em GitHub: Melhores práticas de segurança para AWS WAF.

Modelos de exemplo com ação de correção

Melhores práticas operacionais para o Amazon DynamoDB com remediação

O modelo está disponível em GitHub: Melhores práticas operacionais para o Amazon DynamoDB com remediação.

Melhores práticas operacionais para o Amazon S3 com remediação

O modelo está disponível em GitHub: Melhores práticas operacionais para o Amazon S3 com remediação.

Para obter mais informações sobre a estrutura do modelo, consulte Anatomia do modelo no Guia do AWS CloudFormation usuário.

Pacotes de conformidade personalizados

Um pacote de conformidade personalizado é uma coleção exclusiva de AWS Config regras e ações de remediação que você pode implantar juntas em uma conta e uma AWS região, ou em uma organização em. AWS Organizations

Para criar um pacote de conformidade personalizado, siga as etapas na seção Personalização do modelo a seguir para criar um arquivo YAML que contenha a lista de Regras gerenciadas do AWS Config ou Regras personalizadas do AWS Config com as quais você deseja trabalhar.

Terminologia

AWS Config As regras gerenciadas são regras predefinidas de propriedade AWS Config da.

AWS Config Regras personalizadas são regras que você cria do zero.

Há duas maneiras de criar regras AWS Config personalizadas: com as funções Lambda (Guia do AWS Lambda desenvolvedor) e com o Guard (Guard GitHub Repository), uma linguagem. policy-as-code AWS Config as regras personalizadas criadas com AWS Lambda são chamadas de Regras

Lambda AWS Config Personalizadas e as regras AWS Config personalizadas criadas com o Guard são chamadas de Regras de Política AWS Config Personalizadas.

Personalizar o modelo

Criar seu arquivo YAML

Para criar um arquivo YAML, abra um editor de texto e salve o arquivo como .yaml.

> **Note**
>
> Seu arquivo conterá uma seção de Parâmetros e Recursos.

Parâmetros

A `Parameters` seção em seu arquivo YAML é para os parâmetros de regra do conjunto de AWS Config regras que você adicionará posteriormente na `Resources` seção. Crie a seção `Parameters` copiando e colando o seguinte bloco de código em seu arquivo YAML, personalizando-o conforme necessário e repetindo para cada parâmetro de regra.

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

Por exemplo: .

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> Ao selecionar as AWS Config Regras para criar seu pacote de conformidade personalizado, verifique se você tem os recursos provisionados em sua conta que serão avaliados de acordo com as Regras. AWS Config

1. A primeira linha na seção de parâmetros depois `Parameters:` é uma string concatenada de *`NameOfRule`*+ Param +. *`NameOfRuleParameter`*

   a. Substitua *`NameOfRule`* por um nome consistente criado por você para a regra. Por exemplo, isso pode ser IamPasswordPolicypara a iam-password-policy regra.

   b. Digite `Param`.

   c. Em seguida, substitua *`NameOfRuleParameter`* pelo nome do parâmetro da regra para sua regra específica. Para Regras AWS Config gerenciadas, o nome do parâmetro da regra está localizado na Lista de regras AWS Config gerenciadas (por exemplo, MinimumPasswordLengthé o nome de um parâmetro de regra para a iam-password-policyregra). Para regras do AWS Config personalizadas, o nome do parâmetro da regra é o nome que você escolheu ao criar a regra.

2. Se você estiver usando uma regra AWS Config gerenciada, encontre a AWS Config regra apropriada na lista de regras gerenciadas para saber os valores aceitos para `Default` e `Type` para sua regra específica. Para regras do AWS Config personalizadas, use os valores selecionados ao criar a regra.

> **Note**
>
> Para cada parâmetro, `Type` deve ser especificado. `Type`pode ser “String”, “int”, “double”, “CSV”, “boolean” e "StringMap”.

Recursos do

A seção `Resources` lista as regras que estão sendo adicionadas ao seu pacote de conformidade personalizado. Adicione o bloco `Resources` a seguir diretamente abaixo de sua seção `Parameters`, personalizando-o, conforme necessário, e repetindo para cada regra. Para obter mais informações sobre as especificações, consulte AWS::Config::ConfigRule.

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
```

```
        Type: AWS::Config::ConfigRule
    ...
```

Por exemplo: .

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> Ao selecionar as AWS Config regras para criar seu pacote de conformidade personalizado, verifique se você tem os recursos que serão avaliados para as AWS Config regras provisionadas em sua conta. Para obter mais informações, consulte Tipos de Recursos Compatíveis.

1. Substitua *`NameOfRule`* pelo mesmo nome que você criou na seção `Parameters`.
2. Para Regras AWS Config gerenciadas, *`ActualConfigRuleName`* substitua pelo título da página de regras apropriada na Lista de regras AWS Config gerenciadas. Para regras AWS Config personalizadas, use o nome da regra de configuração que você escolheu no momento da criação da regra.
3. Substitua *`NameOfRuleParameter`* pelo mesmo nome que você usou na seção `Parameters`. Depois dos dois pontos, copie e cole a mesma sequência concatenada de *`NameOfRule`*+ Param + *`NameOfRuleParameter`*que você criou na seção. `Parameters`
4. Altere o *`Owner`* para o valor apropriado.

> **Note**
>
> AWS Config Regras gerenciadas

Para regras AWS Config gerenciadas, o valor de `Owner` seráAWS.

AWS Config Regras personalizadas

Para regras AWS Config personalizadas criadas com o Guard, o valor de `Owner` seráCUSTOM_POLICY. Para regras AWS Config personalizadas criadas com o Lambda, o valor de `Owner` será. CUSTOM_LAMBDA

5. Altere o *`SOURCE_IDENTIFIER`* para o valor apropriado.

> **Note**
>
> AWS Config Regras gerenciadas
>
> Para Regras AWS Config Gerenciadas, copie o identificador seguindo o link da regra selecionada na Lista de Regras AWS Config Gerenciadas (por exemplo, o identificador de origem da access-keys-rotatedregra é ACCESS_KEYS_ROTATED).
>
> AWS Config Regras personalizadas
>
> Para regras AWS Config personalizadas criadas com o Lambda, `SourceIdentifier` é o Amazon Resource Name (ARN) da AWS Lambda função da regra, como. `arn:aws:lambda:us-east-2:123456789012:function:`*`ActualConfigRuleName`* Para regras AWS Config personalizadas criadas com o Guard, esse campo não é necessário.

No geral, seu pacote de conformidade personalizado preenchido deve começar a ter uma aparência semelhante ao seguinte, que é um exemplo usando essas regras AWS Config gerenciadas: iam-password-policyaccess-keys-rotated, e -check. iam-user-unused-credentials

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
```

```
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge:
IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

Implantar seu pacote de conformidade personalizado

Para implantar seu pacote de conformidade personalizado, consulte Implantando um pacote de conformidade usando o AWS Config console e a implantação de um pacote de conformidade usando a interface de AWS Config linha de comando.

Visualizar dados de conformidade no painel de controle dos pacotes de conformidade

A página principal dos Pacotes de Conformidade exibe todos os pacotes de conformidade que você tem atualmente na sua Conta da AWS. A página também contém o nome, o status da implantação e a pontuação de conformidade de cada pacote de conformidade. A pontuação de conformidade é a porcentagem do número de combinações de recursos e regras compatíveis em um pacote de conformidade em comparação com o número total de combinações possíveis de regras e recursos.

Você pode usar esse painel para entender o nível de conformidade de seus pacotes de conformidade e usar a pontuação de conformidade para monitorar o progresso da correção, realizar comparações entre diferentes conjuntos de requisitos e ver o impacto que uma alteração ou implantação específica tem em um pacote de conformidade.

Navegar pela página principal dos pacotes de conformidade

1. Faça login no AWS Management Console e abra o console do AWS Config em https://console.aws.amazon.com/config/.
2. Navegue até a página Pacotes de conformidade. Analise seus pacotes de conformidade e sua pontuação de conformidade. Você também pode fazer o seguinte:
   - Para adicionar e configurar um novo pacote de conformidade, escolha Implantar pacote de conformidade.
   - Para excluir um pacote de conformidade e seus dados, altere as configurações ou visualize detalhes adicionais, como o local de entrega ou os parâmetros, escolha um pacote de conformidade e escolha Ações.

     > **Note**
     >
     > Não é possível editar um pacote de conformidade implantado. Você pode modificar as outras seleções a qualquer momento escolhendo o nome do pacote de conformidade e Editar no menu suspenso Ações.

   - Para ver o histórico das alterações do estado de conformidade, escolha um pacote de conformidade e escolha o Cronograma do pacote de conformidade. Para obter mais informações, consulte Viewing the Compliance History Timeline for Conformance Packs.
   - Para visualizar o status da implantação, a pontuação de conformidade, o cronograma da pontuação de conformidade e as regras de um pacote de conformidade em uma exibição detalhada, selecione um pacote de conformidade e escolha Exibir.

Saiba mais

Pré-requisitos do pacote de conformidade

Modelos de exemplo de pacote de conformidade

Implantar um pacote de conformidade

Limites de serviço da AWS

Visualizar o cronograma do histórico de conformidade dos pacotes de conformidade

AWS Config suporta o armazenamento de alterações do estado de conformidade em seus pacotes de conformidade. Isso permite que você visualize o histórico das alterações do estado de conformidade. Essas alterações no estado de conformidade são apresentadas como um cronograma. O cronograma captura alterações como `ConfigurationItems` ao longo de um período. Você também pode usar esse recurso para encontrar regras específicas em um pacote de conformidade que não estejam em conformidade.

Você pode aceitar ou cancelar o registro de todos os tipos de recurso no AWS Config. Se você optou por registrar todos os tipos de recursos, começará AWS Config automaticamente a registrar o histórico de conformidade do pacote de conformidade, conforme avaliado pelas Regras. AWS Config Por padrão, AWS Config registra as alterações de configuração de todos os recursos suportados. Você também pode selecionar apenas o tipo de recurso específico do histórico de conformidade do pacote de conformidade: `AWS::Config::ConformancePackCompliance`. A gravação do tipo de recurso `AWS::Config::ConformancePackCompliance` está disponível sem custo adicional. Para obter mais informações, consulte Selecionar quais AWS Config registros de recursos.

Um pacote de conformidade é compatível se todas as regras em um pacote de conformidade estiverem em conformidade. Não está em conformidade, se alguma das regras não estiver em conformidade. O status de conformidade de um pacote de conformidade é INSUFFICIENT_DATA somente se todas as regras dentro de um pacote de conformidade não puderem ser avaliadas devido a dados insuficientes. Se algumas das regras em um pacote de conformidade forem compatíveis, mas o status de conformidade de outras regras nesse mesmo pacote de conformidade for INSUFFICIENT_DATA, o pacote de conformidade mostrará conformidade. A conformidade de um pacote de conformidade não é avaliada de uma só vez. Algumas regras podem levar mais tempo para serem avaliadas do que outras. A conformidade é avaliada para grupos de regras por vez, continuando em etapas até que todas as regras em um pacote de conformidade tenham sido avaliadas.

Tópicos

- Visualizar o cronograma de conformidade
- Consultar histórico de conformidade

Visualizar o cronograma de conformidade

Acesse o cronograma de conformidade selecionando um pacote de conformidade específico na página principal do pacote de conformidade.

1. Navegue até a página do Pacote de conformidade.
2. Na página principal do Pacote de conformidade, escolha um pacote de conformidade específico e, em seguida, escolha o Cronograma do pacote de conformidade.

> **Note**
>
> Como alternativa, você pode usar o cronograma de conformidade na página de detalhes do pacote de conformidade. Selecione um pacote de conformidade e escolha Visualizar detalhes no menu suspenso Ações. Nessa página, escolha Cronograma do pacote de conformidade.

O cronograma mostra o histórico das alterações no estado de conformidade de um pacote de conformidade. Você pode fazer o seguinte:

1. Expanda uma alteração de conformidade para ver o status de line-by-line conformidade de cada regra em um pacote de conformidade.
2. Na exibição expandida, escolha uma regra específica para ver sua página de detalhes.

Consultar histórico de conformidade

Consulte o histórico de conformidade get-resource-config-history usando o tipo de recurso`AWS::Config::ConformancePackCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

Você deve ver saída semelhante a:

```
{
    "configurationItems": [
        {
            "version": "1.3",
```

```
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
```

```
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

Para obter mais informações, consulte Tipos de recursos compatíveis (AWS Config) e GetResourceConfigHistoryna referência da API.

Implantar um pacote de conformidade usando o console do AWS Config

Na página Conformance packs (Pacotes de conformidade), é possível implantar um pacote de conformidade em uma conta em uma região. Também é possível editar e excluir o pacote de conformidade implantado.

Implante um pacote de conformidade usando modelos

Você pode implantar um pacote de conformidade usando modelos de AWS Config amostra ou seu próprio modelo personalizado. Para obter instruções sobre como criar pacotes de conformidade personalizados, consulte Pacote de conformidade personalizado.

1. Faça login no AWS Management Console e abra o console do AWS Config em https://console.aws.amazon.com/config/.
2. Navegue até a página Conformance packs (Pacotes de conformidade) e escolha Deploy conformance pack (Implantar pacote de conformidade).
3. Na página Specify template (Especificar modelo) escolha um modelo de exemplo ou use um modelo existente. Para obter mais informações, consulte Modelos de amostra de conformidade.
   - Se você escolher Usar modelo de amostra, selecione um modelo de amostra na lista suspensa de modelos de amostra.

Para obter informações sobre o conteúdo de cada modelo, consulte Modelos de exemplo de pacote de conformidade.

- Se você selecionar Template is ready (O modelo está pronto), especifique a origem do modelo. É um URI do Amazon S3, um AWS Systems Manager documento (documento SSM) ou um modelo que você carrega.

  Se o modelo tiver mais de 50 KB, faça upload dele no bucket do S3 e selecione esse local do bucket do S3. Por exemplo: s3://*bucketname/prefix*.

  > **Important**
  >
  > Escolher modelo está pronto se você criou seu arquivo YAML do pacote de conformidade do zero com base no Pacote de Conformidade Personalizado.

4. Escolha Próximo.
5. Na página Specify conformance pack details (Especificar detalhes do pacote de conformidade) digite o nome do pacote de conformidade.

   O nome do pacote de conformidade deve ser um nome exclusivo com no máximo 256 caracteres alfanuméricos. O nome pode conter hífens, mas não pode conter espaços.
6. Opcional: adicione um parâmetro.

   Os parâmetros são definidos em seu modelo e ajudam você a gerenciar e organizar os recursos.
7. Escolha Próximo.
8. Na página Review and deploy (Revisar e implantar) revise todas as informações.

   É possível editar os detalhes do modelo e os detalhes do pacote de conformidade selecionando Edit (Editar).
9. Escolha Deploy conformance pack (Implantar pacote de conformidade).

   O AWS Config exibe o pacote de conformidade na página do pacote de conformidade com o status apropriado.

   Se a implantação do pacote de conformidade falhar, verifique suas permissões, verifique se você concluiu as etapas de pré-requisito e tente novamente. Ou você pode entrar em contato comAWS Support.

Para implantar um conformance pack using sample template with remediations (pacote de conformidade usando modelo de exemplo com correções), consulte o Pré-requisitos para usar um pacote de conformidade com correção e use o procedimento anterior.

Para implantar um pacote de conformidade com uma ou mais AWS Config regras, consulte o. Pré-requisitos para usar um pacote de conformidade com uma ou mais regras AWS Config

Editar um pacote de conformidade

1. Para editar um pacote de conformidade, selecione o pacote de conformidade na tabela.
2. Escolha Actions (Ações) e escolha Edit (Editar).
3. Na página Edit conformance pack (Editar pacote de conformidade), é possível editar os detalhes do modelo, o modelo de exemplo, o pacote de conformidade e a seção de parâmetros.

   Não é possível alterar o nome do pacote de conformidade.
4. Escolha Salvar alterações.

   O pacote de conformidade é exibido com as regras do AWS Config.

Excluir um pacote de conformidade

1. Para excluir um pacote de conformidade, selecione o pacote de conformidade na tabela.
2. Escolha Actions e, em seguida, escolha Delete.
3. Na caixa de diálogo excluir `pacote de conformidade`, confirme se você deseja excluir permanentemente esse pacote de conformidade.

   > **Important**
   >
   > Essa ação não poderá ser revertida. Ao excluir um pacote de conformidade, você exclui todas as regras do AWS Config e as ações de correção nesse pacote de conformidade.
4. Insira Delete e escolha Delete (Excluir).

   Na página Conformance packs (Pacotes de conformidade), você verá o status da implantação como Deleting (Excluindo) até que o pacote de conformidade seja excluído totalmente.

Implantar um pacote de conformidade usando a AWS Command Line Interface

Você pode implantar, visualizar, atualizar, visualizar o status de conformidade e excluir um pacote de AWS Config conformidade usando o AWS Command Line Interface ()AWS CLI.

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, digite `aws configure` para configurar o AWS CLI para usar uma AWS região em que os pacotes de conformidade estejam disponíveis.

Tópicos

- Implantar um pacote de conformidade
- Visualizar um pacote de conformidade
- Visualizar o status do pacote de conformidade
- Visualizar o status de conformidade do pacote de conformidade
- Obter detalhes de conformidade de um pacote de conformidade específico
- Excluir um pacote de conformidade

Implantar um pacote de conformidade

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite um dos comandos a seguir para implantar um pacote de conformidade chamado **`MyConformancePack`**. A fonte do modelo é um URI do Amazon S3, um modelo que você carrega ou um AWS Systems Manager documento (documento SSM).

   URI do Amazon S3

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-s3-uri "s3://AmazonS3BucketName/templateName.yaml"
--delivery-s3-bucket AmazonS3BucketName
```

Modelo YAML do seu diretório local

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-body template body
```

AWS Systems Manager Documento (documento do Systems Manager)

```
aws configservice put-conformance-pack
--conformance-pack-name MyConformancePack
--template-ssm-document-details
 DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
--delivery-s3-bucket AmazonS3BucketName
```

3. Pressione Enter para executar o comando.

   Você deve ver saída semelhante ao seguinte:

```
{
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID"
}
```

> **Note**
>
> Para obter mais informações sobre como criar um modelo da YAML para um pacote de conformidade, consulte Custom Conformance Pack.

Visualizar um pacote de conformidade

1. Insira o comando da a seguir.

```
aws configservice describe-conformance-packs
```

OU

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. Você deve ver saída semelhante ao seguinte:

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

Visualizar o status do pacote de conformidade

1. Insira o comando da a seguir.

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. Você deve ver saída semelhante ao seguinte:

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

Visualizar o status de conformidade do pacote de conformidade

1. Insira o comando da a seguir.

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. Você deve ver saída semelhante ao seguinte:

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
        }
    ]
}
```

Obter detalhes de conformidade de um pacote de conformidade específico

1. Insira o comando da a seguir.

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. Você deve ver saída semelhante ao seguinte:

```
{
    "conformancePackRuleEvaluationResults": [
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
```

```
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

Excluir um pacote de conformidade

Insira o comando da a seguir.

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

Se for bem sucedido, o comando será executado sem saída adicional.

> **Important**
>
> Essa ação não poderá ser revertida. Ao excluir um pacote de conformidade, você exclui todas as AWS Config regras e ações de remediação desse pacote de conformidade.

Gerenciar pacotes de conformidade (API)

Use as seguintes ações de AWS Config API para gerenciar pacotes de conformidade:

- DeleteConformancePacote, exclui o pacote de conformidade especificado e todas as AWS Config regras e todos os resultados da avaliação dentro desse pacote de conformidade.
- DescribeConformancePackCompliance, retorna as informações de conformidade de cada regra desse pacote de conformidade.
- DescribeConformancePacotes, retorna uma lista de um ou mais pacotes de conformidade.
- DescribeConformancePackStatus, fornece o status de implantação de um ou mais pacotes de conformidade.
- GetConformancePackComplianceDetalhes, retorna os detalhes de conformidade de um pacote de conformidade para todos os AWS recursos que são monitorados pelo pacote de conformidade.
- GetConformancePackComplianceResumo, retorna as informações de conformidade do pacote de conformidade com base nos resultados cumulativos de conformidade de todas as regras desse pacote de conformidade.
- ListConformancePackCompliancePontuações, retorna uma lista das pontuações de conformidade do pacote de conformidade.
- PutConformanceEmpacota, cria ou atualiza um pacote de conformidade.

Gerenciar pacotes de conformidade em todas as contas na organização

Use AWS Config para gerenciar pacotes de conformidade em toda a Contas da AWS organização. Você pode fazer o seguinte:

- Implantar, atualizar e excluir pacotes de conformidade de forma centralizada em todas as contas-membro de uma organização no AWS Organizations.
- Implante um conjunto comum de AWS Config regras e ações de remediação em todas as contas e especifique as contas nas quais AWS Config as regras e ações de remediação não devem ser criadas.
- Use a conta de gerenciamento AWS Organizations para impor a governança, garantindo que AWS Config as regras subjacentes e as ações de remediação não possam ser modificadas pelas contas dos membros de sua organização.

Considerações

Para implantações em diferentes regiões

A chamada de API para implantar regras e pacotes de conformidade em todas as contas é AWS específica da região. No nível da organização, você precisa alterar o contexto da sua chamada de API para uma região diferente se quiser implantar regras em outras regiões. Por exemplo, para implantar uma regra no Leste dos EUA (Norte da Virgínia), altere a região para Leste dos EUA (Norte da Virgínia) e depois chame `PutOrganizationConfigRule`.

Para contas dentro de uma organização

Se uma nova conta entrar em uma organização, o pacote de regras ou conformidade será implantado nessa conta. Quando uma conta sai de uma organização, o pacote de regras ou conformidade é removido.

Se você implantar uma regra organizacional ou pacote de conformidade em uma conta de administrador da organização e, em seguida, estabelecer um administrador delegado e implantar uma regra organizacional ou pacote de conformidade na conta do administrador delegado, você não poderá ver a regra organizacional ou o pacote de conformidade na conta do administrador da organização a partir da conta do administrador delegado ou ver a regra organizacional ou o pacote de conformidade na conta do administrador delegado da conta do administrador da organização. As DescribeOrganizationConformancePacksAPIs DescribeOrganizationConfigRulese só podem ver e interagir com os recursos relacionados à organização que foram implantados de dentro da conta que chama essas APIs.

Mecanismo de repetição para novas contas adicionadas a uma organização

A implantação de regras organizacionais e pacotes de conformidade existentes só será repetida por sete horas após a adição de uma conta à sua organização se um gravador não estiver disponível. Espera-se que você crie um gravador, se não houver um dentro de sete horas após a adição de uma conta à sua organização.

Contas de gerenciamento da organização, administradores delegados e funções vinculadas a serviços

Se você estiver usando uma conta de gerenciamento da organização e pretende usar um administrador delegado para implantação organizacional, saiba que AWS Config não criará automaticamente a função vinculada ao serviço (SLR). Você deve criar manualmente a função vinculada ao serviço (SLR) separadamente usando o IAM.

Se você não tiver uma SLR para sua conta de gerenciamento, não poderá implantar recursos nessa conta a partir de uma conta de administrador delegado. Você ainda poderá implantar pacotes de conformidade nas contas dos membros a partir das contas de gerenciamento e de administrador delegado. Para obter mais informações, consulte Como usar funções vinculadas ao serviço no Guia do usuário AWS Identity and Access Management (IAM).

Implantação

To deploy with the AWS Management Console

Para implantar um pacote de conformidade em uma organização a partir do AWS console, use. AWS Systems ManagerPara obter mais informações, consulte Implantar pacotes de AWS Config conformidade no Guia do AWS Systems Manager usuário.

To deploy with the AWS API

Para obter informações sobre como integrar AWS Config com AWS Organizations, consulte AWS Config e AWS Organizations no Guia do AWS Organizations usuário. Certifique-se AWS Config de que a gravação esteja ativada antes de usar as seguintes APIs para gerenciar as regras do pacote de conformidade em toda a Contas da AWS organização:

- DeleteOrganizationConformancePack, exclui o pacote de conformidade da organização especificado e todas as regras de configuração e ações de remediação de todas as contas membros dessa organização.
- DescribeOrganizationConformancePacks, retorna uma lista de pacotes de conformidade organizacional.
- DescribeOrganizationConformancePackStatus, fornece o status de implantação do pacote de conformidade organizacional para uma organização.
- GetOrganizationConformancePackDetailedStatus, retorna o status detalhado de cada conta membro dentro de uma organização para um determinado pacote de conformidade da organização.
- PutOrganizationConformancePack, implanta pacotes de conformidade em todas as contas dos membros em uma organização. AWS

Suporte regional

A implantação de pacotes de conformidade nas contas dos membros de uma AWS organização é suportada nas seguintes regiões.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (N. da Califórnia)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Solução de problemas

Status de falha em um pacote de conformidade

Se você receber um erro indicando que o pacote de conformidade falhou durante a criação, a atualização ou a exclusão, verifique o status do pacote de conformidade.

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

Você deve ver saída semelhante ao seguinte:

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
        "ConformancePackStatusReason": "Failure Reason",
```

```
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

Verifique o ConformancePackStatusReasonpara obter informações sobre a falha.

When the stackArn is present in the response (Quando o stackArn está presente na resposta)

Se a mensagem de erro não estiver clara ou se a falha for por causa de um erro interno, acesse o console do AWS CloudFormation e faça o seguinte:

1. Procure o stackArn da saída.
2. Escolha a guia Eventos da CloudFormation pilha e verifique se há eventos com falha.

   O motivo do status indica por que o pacote de conformidade falhou.

When the stackArn is not present in the response (Quando o stackArn não está presente na resposta)

Se você receber uma falha ao criar um pacote de conformidade, mas o StackArn não estiver presente na resposta de status, o possível motivo é que a criação da pilha falhou, reverteu e excluiu a pilha. CloudFormation Acesse o CloudFormation console e pesquise as pilhas que estão no estado Excluído. A pilha com falha pode estar disponível lá. A CloudFormation pilha contém o nome do pacote de conformidade. Se você encontrar a pilha com falha, escolha a guia Eventos da CloudFormation pilha e verifique se há eventos com falha.

Se nenhuma dessas etapas funcionou e se o motivo da falha for um erro interno do serviço, tente operar novamente ou entre em contato com o AWS Support Centro.

Regras pendentes em um pacote de conformidade

A implantação de um pacote de conformidade envolve a criação de uma AWS CloudFormation pilha subjacente em segundo plano para implantar as regras no modelo do pacote de conformidade. Essas regras são regras vinculadas a serviços e não podem ser atualizadas ou excluídas fora do pacote de conformidade.

Se você fizer alterações na CloudFormation pilha subjacente, isso resultará em uma situação em que o pacote de conformidade e suas regras se tornarão incontroláveis. Essas regras incontroláveis são regras pendentes.

Deslize entre a CloudFormation pilha e o pacote de conformidade

Você pode atualizar os nomes das regras em um modelo de pacote de conformidade diretamente do CloudFormation console. Se você atualizar o modelo diretamente do CloudFormation console, isso não atualizará o pacote de conformidade implantado.

Esse desvio cria uma regra de oscilação. Se você tentar excluir a regra do pacote de conformidade, receberá um erro semelhante ao seguinte:

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

Se você tentar excluir o pacote de conformidade, a regra pendente não poderá ser excluída e você receberá um erro semelhante ao seguinte:

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

Para corrigir esse problema, execute as seguintes etapas:

1. Exclua a pilha . Para obter mais informações, consulte Excluindo uma pilha no AWS CloudFormation console no Guia do CloudFormation usuário.
2. Exclua o pacote de conformidade usando o AWS Config console ou usando a API DeleteConformancePack. Se for um pacote de conformidade organizacional e você estiver usando a conta de gerenciamento ou de administrador delegado, use a API. DeleteOrganizationConformancePack
3. Entre em contato com o AWS Support Centro com o Amazon Resource Name (ARN) das regras pendentes no pacote de conformidade para ajudar a limpar sua conta.

Para evitar esse problema, lembre-se destas práticas recomendadas:

- Nunca faça nenhuma atualização direta na CloudFormation pilha de um pacote de conformidade.
- Nunca tente fazer alterações que criem um desvio entre o pacote de conformidade e sua pilha subjacente. CloudFormation
- A função vinculada ao serviço (SLR) dos pacotes de conformidade não pode ser modificada. Verifique se os recursos que você está atualizando fazem parte da política de permissões da SLR.

CloudFormation Pilha excluída de um pacote de conformidade

A menos que haja um desvio entre a CloudFormation pilha e o pacote de conformidade, nunca é recomendável excluir as regras em um pacote de conformidade ou em sua CloudFormation pilha diretamente do console. CloudFormation

Para corrigir esse problema, entre em contato com o AWS Support Centro com o Amazon Resource Name (ARN) das regras pendentes no pacote de conformidade para ajudar a limpar sua conta.

Para evitar esse problema, lembre-se destas práticas recomendadas:

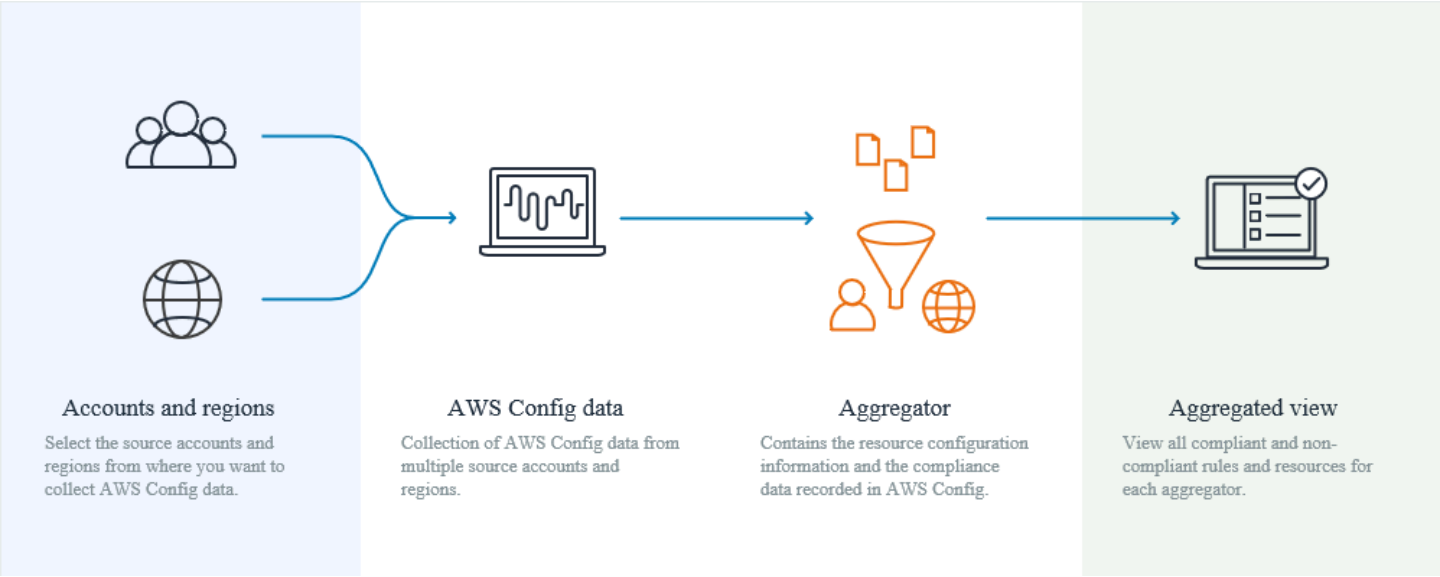
- Nunca exclua a CloudFormation pilha subjacente de um pacote de conformidade.
- Exclua pacotes de conformidade usando a API Pack. DeleteConformance Se for um pacote de conformidade organizacional e você estiver usando a conta de gerenciamento ou de administrador delegado, use a API. DeleteOrganizationConformancePack

Agregação de dados de várias regiões e várias contas

Um agregador é um tipo de AWS Config recurso que coleta dados AWS Config de configuração e conformidade do seguinte:

- Várias contas e várias AWS regiões.
- Conta única e várias AWS regiões.
- Uma organização AWS Organizations e todas as contas dessa organização que foram AWS Config ativadas.

Use um agregador para visualizar a configuração de recursos e os dados de conformidade registrados no AWS Config. Um agregador usa um bucket do Amazon S3 para armazenar dados agregados. Ele recupera periodicamente os instantâneos de configuração das contas de origem e os armazena no bucket S3 designado. A imagem a seguir mostra como um agregador coleta AWS Config dados de várias contas e regiões.



Casos de uso

- Monitoramento de conformidade: você pode agregar dados de conformidade para avaliar as posturas gerais de conformidade da sua organização ou de todas as contas e regiões.
- Rastreamento de alterações: você pode acompanhar as alterações nos recursos ao longo do tempo em toda a sua organização ou em todas as contas e regiões.

- Relacionamentos de recursos: você pode analisar dependências e relacionamentos de recursos em toda a sua organização ou entre contas e regiões.

> **Note**
>
> Os agregadores fornecem uma visão somente para leitura das contas e regiões de origem que o agregador está autorizado a visualizar, replicando dados das contas de origem na conta do agregador. Os agregadores não fornecem acesso mutável a uma conta ou região de origem. Por exemplo, isso significa que você não pode implantar regras por meio de um agregador ou enviar arquivos de instantâneos para uma conta ou região de origem por meio de um agregador.
> O uso de agregadores não incorre em custos adicionais.

Terminologia

Uma conta de origem é a Conta da AWS partir da qual você deseja agregar dados de configuração e conformidade de AWS Config recursos. Uma conta de origem pode ser uma conta individual ou uma organização no AWS Organizations. Você pode fornecer contas de origem individualmente ou recuperá-las por meio AWS Organizations de.

Uma região de origem é a AWS região da qual você deseja agregar dados de AWS Config configuração e conformidade.

Uma conta agregadora é uma conta na qual você cria um agregador.

A autorização se refere às permissões que você concede a uma conta agregadora e a uma região para coletar seus dados AWS Config de configuração e conformidade. A autorização não é necessária se você estiver agregando contas de origem que fazem parte do AWS Organizations.

Como agregar dados

Para agregar seus AWS Config dados das contas e regiões de origem, comece com:

1. Adicionar um agregador para agregar dados AWS Config de configuração e conformidade de várias contas e regiões. Para obter mais informações, consulte Configurar um agregador usando o console e Configurando um agregador usando o AWS Command Line Interface.

2. Autorizar contas agregadoras a coletar dados de AWS Config configuração e conformidade. Para obter mais informações, consulte Autorizando contas agregadoras a coletar dados AWS Config de configuração e conformidade usando o console e Autorizando contas agregadoras a coletar dados AWS Config de configuração e conformidade usando o AWS Command Line Interface.

> **Note**
>
> Há dois tipos de agregadores: agregador de contas individuais e agregador da organização
>
> Para o agregador de contas individuais, a autorização é necessária para todas as regiões incluídas da conta de origem, incluindo regiões externas da conta ou regiões da conta membro da organização.
>
> Para o agregador da organização, a autorização não é necessária para as regiões da conta dos membros da organização, pois a autorização é integrada ao serviço Organizations.

3. Monitorar dados de conformidade para regras e contas na visualização agregada. Para ter mais informações, consulte Como visualizar dados de conformidade e inventário no painel do agregador.

Suporte regional

Atualmente, a agregação de dados multirregional de várias contas é suportada nas seguintes regiões:

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo	
Oeste dos EUA (Norte da Califórnia)	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
África (Cidade do Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
Ásia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milão)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
Europa (Espanha)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurique)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	config.me-central-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Solução de problemas para agregação de dados multirregionais de várias contas

AWS Config pode não agregar dados das contas de origem por um dos seguintes motivos:

Se isso acontecer	Faça o seguinte
AWS Config não está habilitado na conta de origem para contas dentro de uma organização.	Ative AWS Config a conta de origem e autorize a conta agregadora a coletar dados.
A autorização não é concedida a uma conta de agregador.	Faça login na conta de origem e conceda autorização à conta agregadora para coletar AWS Config dados.
Pode haver um problema temporário que impede a agregação de dados.	A agregação de dados está sujeita a atrasos. Aguarde alguns minutos.

AWS Config pode não agregar dados de uma organização por um dos seguintes motivos:

Se isso acontecer	Faça o seguinte
AWS Config não consegue acessar os detalhes da sua organização devido à função inválida do IAM.	Crie um perfil do IAM ou selecione um válido na lista de perfis do IAM. **Note** Se a função do IAM for inválida por mais de 24 horas, AWS Config excluirá os dados de toda a organização.
AWS Config o acesso ao serviço está desativado em sua organização.	Você pode ativar a integração entre AWS Config e AWS Organizations por meio da `EnableAWS ServiceAccess` API. Se você escolher Adicionar minha organização no console, AWS Config habilitará automaticamente a integração entre AWS Config AWS Organizations e.
AWS Config não consegue acessar os detalhes da sua organização porque todos os recursos não estão habilitad os na sua organização.	Ative todos os recursos no AWS Organizations console.
As alterações organizacionais, como: adicionar uma conta, remover uma conta, habilitar o acesso ao serviço e desabilitar o acesso ao serviço, não são atualizadas imediatamente nas regiões do Oriente Médio (Bahrein) e Ásia-Pacífico (Hong Kong).	As alterações organizacionais estão sujeitas a um atraso de duas horas. Aguarde duas horas para ver todas as alterações na organização.

Como visualizar dados de conformidade e inventário no painel do agregador

O painel na página Agregadores exibe os dados de configuração dos seus recursos agregados AWS . Ele fornece uma visão geral de suas regras, pacotes de conformidade e seus estados de conformidade.

O painel fornece a contagem total de AWS recursos. Os tipos de recursos e contas de origem são classificadas pelo maior número de recursos. Isso também exibe uma contagem de regras compatíveis e não compatíveis. As regras não compatíveis são classificadas pelo maior número de recursos não compatíveis. Os pacotes de conformidade e as contas de origem não compatíveis são classificados pelo maior número de regras não compatíveis.

Após a configuração AWS Config, ele começa a agregar dados das contas de origem especificadas em um agregador. Pode demorar alguns minutos para que o status de conformidade das regras seja exibido.

Usando o Painel do Agregador

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Navegue até a página Agregadores. Você pode ver:
   - Suas regras e seus estados de conformidade.
   - Seus pacotes de conformidade e seus estados de conformidade.
   - Seus AWS recursos e seus dados de configuração.
3. Escolha um agregador no painel. Filtre seus agregadores pelo nome do agregador. Você pode visualizar os seguintes widgets:
   - Inventário de recursos

     Visualize os 10 principais tipos de recursos do agregador selecionado, em ordem decrescente pela contagem de recursos. Escolha o número total de recursos para o agregador selecionado, exibido entre parênteses após o Inventário de recursos, para ir até a página Recursos agregados, na qual você pode visualizar todos os recursos de um agregador. Como alternativa, escolha um tipo de recurso no widget para acessar a página Recursos agregados, filtrada conforme o tipo de recurso especificado.

- Contas por contagem de recursos

  Visualize as cinco principais contas do agregador selecionado em ordem decrescente, pela contagem de recursos. Escolha uma conta no widget para acessar a página Recursos, filtrada usando a conta especificada.

- Regras não compatíveis

  Veja as cinco principais regras não compatíveis do agregador selecionado, em ordem decrescente de acordo com o número de recursos não compatíveis. Escolha uma regra no widget para acessar a página de detalhes da regra especificada. Escolha Exibir todas as regras não compatíveis para acessar a página Regras agregadas, na qual você pode visualizar todas as regras de um agregador.

- Contas por meio de regras não compatíveis

  Visualize as cinco principais contas do agregador selecionado, em ordem decrescente pelo número de regras não compatíveis. Escolha uma conta no widget para acessar a página Regras agregadas, na qual você pode ver todas as regras de um agregador filtradas usando a conta especificada.

- Contas por pacotes de conformidade não compatíveis

  Visualize as cinco principais contas do agregador selecionado, em ordem decrescente pelo número de pacotes de conformidade não compatíveis. Escolha uma conta no widget para acessar a página agregada do Pacote de Conformidade, na qual é possível ver todos os pacotes de conformidade de um agregador filtrado usando a conta especificada.

4. No painel de navegação à esquerda, escolha uma das seguintes opções no menu suspenso:

   - Painel de conformidade

     Visualize painéis de conformidade automatizados usando os widgets que resumem os insights sobre a conformidade de recursos em seu agregador. Você pode ver dados como os 10 principais tipos de recursos por recursos não compatíveis e os 10 principais pacotes de conformidade em nível de conta por regras não compatíveis. Para obter informações sobre esses gráficos e tabelas, consulte Painéis de conformidade.

   - Pacotes de conformidade

     Veja todos os pacotes de conformidade criados e vinculados aos diferentes Contas da AWS em seu agregador. A página Pacote de Conformidade exibe uma tabela que lista o nome, a região, o ID da conta e o status de conformidade de cada pacote de conformidade.

Nessa página, você pode escolher um pacote de conformidade e Exibir detalhes para ver informações sobre as regras, recursos e o status de conformidade desse pacote.

- Regras

  Veja todas as regras criadas e vinculadas às diferentes contas da AWS em seu agregador. A página Regras exibe uma tabela que lista o nome, o status de conformidade, a região e a conta de cada regra. Nessa página, você pode escolher uma regra e Visualizar detalhes para obter informações, como agregador, região, ID da conta e recursos no escopo.

- Painel de inventário

  Visualize painéis de inventário automatizados usando os widgets que resumem os insights sobre os dados de configuração de recursos em seu agregador. Você pode ver dados como os 10 principais tipos de recursos por contagem de recursos e as 10 principais contas por contagem de recursos. Para obter informações sobre esses gráficos e tabelas, consulte Painéis de inventário.

- Recursos

  Visualize todos os recursos que estão registrados e vinculados às diferentes contas da AWS em seu agregador. Na página Recurso, escolha um recurso e Exibir detalhes para ver seus detalhes, as regras associadas a ele e a configuração atual do recurso. Você também pode ver informações sobre o recurso, como agregador, região, ID da conta, nome do recurso, tipo de recurso e ID do recurso.

- Autorizações

  Visualize e gerencie todas as contas atualmente autorizadas ou com autorização pendente. Na página Autorizações, escolha Adicionar autorização para fornecer acesso a outra conta. Escolha Excluir autorização para revogar o acesso a partir de um ID de conta.

> **Note**
>
> Solução de problemas
>
> Você poderá ver a mensagem A coleta de dados de todas as contas de origem e regiões está incompleta exibida na visão agregada pelos seguintes motivos:
>
> - A transferência de AWS Config regras não compatíveis e dados de configuração de AWS recursos está em andamento.

- AWS Config não consigo encontrar regras que correspondam ao filtro que você aplicou. Selecione a conta ou a região apropriada e tente novamente.

Você pode ver esta mensagem na exibição agregada: A coleta de dados da sua organização está incompleta. Você pode ver os dados abaixo apenas por 24 horas. Isso pode acontecer por um dos seguintes motivos:

- AWS Config não consegue acessar os detalhes da sua organização por causa de uma função do IAM que não é válida. Se o perfil do IAM permanecer inválido por mais de 24 horas, a AWS Config excluirá os dados de toda a organização.
- AWS Config o acesso ao serviço está desativado em sua organização.

Painel de conformidade

Visualize painéis de conformidade automatizados usando widgets que resumem os insights sobre a conformidade de recursos em seu agregador. Esse painel exibe somente regras com resultados de conformidade.

> **Note**
>
> Limitações
>
> Os insights no painel de conformidade são fornecidos pelo recurso Consultas Avançadas do AWS Config, e esse recurso não oferece suporte a estruturas aninhadas nem à descompactação de matrizes aninhadas. Isso significa que o painel de conformidade exibe a conformidade geral de um recurso e não o status de conformidade de cada regra específica que relata um recurso.
>
> Por exemplo, se você verificar o item de configuração (CI) para o tipo de recurso`AWS::Config::ResourceCompliance`, o painel exibirá os resultados de conformidade de todas as regras que relatam esse recurso. Se houver 10 regras que relatam o recurso, 9 delas são COMPATÍVEIS e somente 1 é NÃO COMPATÍVEL, a conformidade geral desse recurso será NÃO COMPATÍVEL.

Resumo de conformidade por recursos

Exibe um gráfico circular comparando o número de recursos compatíveis com recursos não compatíveis do agregador selecionado. Passe o mouse sobre o gráfico para ver o número e a porcentagem exatos de recursos compatíveis e não compatíveis.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

Os 10 principais tipos de recursos por recursos não compatíveis

Exibe um gráfico de barras horizontais comparando até 10 tipos de recursos do agregador selecionado em ordem decrescente pelo número de recursos não compatíveis. Passe o mouse sobre o gráfico para ver o número exato de recursos não compatíveis para cada tipo de recurso.

Os dados exibidos dependem das configurações do gravador de configuração de cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

As 10 principais contas por recursos não compatíveis

As 10 principais contas por recursos não compatíveis exibem um gráfico de barras horizontais comparando até 10 contas do agregador selecionado em ordem decrescente pelo número de recursos não compatíveis. Passe o mouse sobre o gráfico para ver o número exato de recursos não compatíveis de cada conta.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

As 10 principais regiões por recursos não compatíveis

Exibe um gráfico de barras horizontais comparando até 10 regiões em que o agregador selecionado coleta dados em ordem decrescente de acordo com o número de recursos não compatíveis. Passe o mouse sobre o gráfico para ver o número exato de recursos não compatíveis em cada região.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado.

Os 10 principais pacotes de conformidade em nível de conta de acordo com regras não compatíveis

Exibe um gráfico de barras horizontais comparando até 10 pacotes de conformidade em nível de conta do agregador selecionado em ordem decrescente pelo número de regras não compatíveis. Passe o mouse sobre o gráfico para ver a porcentagem de regras compatíveis e não compatíveis para cada pacote de conformidade em nível de conta.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

Os 10 principais pacotes de conformidade em nível organizacional de acordo com regras não compatíveis

Exibe um gráfico de barras horizontais comparando até 10 pacotes de conformidade de nível organizacional do agregador selecionado em ordem decrescente pelo número de regras não compatíveis. Passe o mouse sobre o gráfico para ver a porcentagem de regras compatíveis e não compatíveis em cada pacote de conformidade de nível organizacional.

Os dados exibidos dependem das configurações do gravador de configuração de cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

As 10 principais contas de acordo com regras não compatíveis em todos os pacotes de conformidade

As 10 principais contas por regras não compatíveis em todos os pacotes de conformidade exibem um gráfico de barras horizontais comparando até 10 contas do agregador selecionado em ordem decrescente pelo número de regras não compatíveis em todos os seus pacotes de conformidade. Passe o mouse sobre o gráfico para ver o número exato de regras não compatíveis em cada conta.

Os dados exibidos dependem das configurações do gravador de configuração de cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

Painel de Inventário

Visualize painéis de inventário automatizados usando widgets que resumem insights sobre dados de configuração de recursos em seu agregador.

Os 10 principais tipos de recursos por contagem de recursos

Exibe um gráfico de barras horizontais comparando até 10 tipos de recursos do agregador selecionado em ordem decrescente por contagem de recursos. Passe o mouse sobre o gráfico para ver o número exato de recursos para cada tipo de recurso.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

Contagem de recursos por região

Exibe um gráfico de barras horizontais comparando até 10 regiões nas quais o agregador selecionado coleta dados em ordem decrescente por contagem de recursos. Passe o mouse sobre o gráfico para ver o número exato de recursos para cada região.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado.

As 10 principais contas por contagem de recursos

Exibe um gráfico de barras horizontais comparando até 10 contas do agregador selecionado em ordem decrescente por contagem de recursos. Passe o mouse sobre o gráfico para ver o número exato de recursos para cada tipo de recurso.

Os dados exibidos dependem das configurações do gravador de configuração de cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados.

Contagem de recursos por tipos de recursos de serviço do Amazon EC2

Exibe um gráfico de barras horizontais comparando os tipos de recursos do Amazon EC2 do agregador selecionado em ordem decrescente por contagem de recursos. Passe o mouse sobre o gráfico para ver o número exato de recursos para cada tipo de recurso do Amazon EC2.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados. Para usar esse gráfico, você deve configurar o gravador para registrar os tipos de recursos do Amazon EC2. Para obter mais informações, consulte Selecionar quais AWS Config registros de recursos.

Os 10 principais tipos de instância do EC2 usados

Exibe um gráfico de barras horizontais comparando até 10 tipos de instância do Amazon EC2 do agregador selecionado em ordem decrescente por uso. Passe o mouse sobre o gráfico para ver o uso de cada tipo de instância do EC2.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados. Para usar esse gráfico, você deve configurar o gravador para registrar o tipo de recurso da instância EC2. Para obter mais informações, consulte AWS Recursos de recodificação.

Contagens de volume do EBS por tipo e tamanho de volume

Exibe um gráfico de barras verticais comparando os volumes do EBS do agregador selecionado por contagem de recursos. Passe o mouse sobre o gráfico para ver o detalhamento da contagem e do tamanho de cada tipo de volume do EBS.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados. Para usar esse gráfico, você deve configurar o gravador para registrar o tipo de recurso de volume EC2. Para obter mais informações, consulte Selecionar quais AWS Config registros de recursos.

Número de instâncias do EC2 em execução versus interrompidas por tipo

Exibe um gráfico de barras horizontais comparando os tipos de instância do EC2 do agregador selecionado que estão em execução com as instâncias do EC2 que foram interrompidas por tipo de instância. Passe o mouse sobre o gráfico para ver o número exato de instâncias do EC2 interrompidas e em execução para cada tipo.

Os dados exibidos dependem das configurações do gravador de configuração para cada conta no agregador selecionado e das regiões em que o agregador selecionado está configurado para coletar dados. Para usar esse gráfico, você deve configurar o gravador para registrar o tipo de recurso da instância EC2. Para obter mais informações, consulte AWS Recursos de recodificação.

Configurar um agregador usando o console

Na página Aggregator (Agregador), você pode fazer o seguinte:

- Crie um agregador especificando os IDs da conta de origem ou a organização e as regiões a partir das quais você deseja agregar dados.
- Editar e excluir um agregador.

Tópicos

- Criar um agregador
- Editar um agregador
- Excluir um agregador

Criar um agregador

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Navegue até a página Agregadores e escolha Adicionar agregador.
3. Permite a replicação de dados, dá permissão AWS Config para replicar dados das contas de origem em uma conta agregadora.

   Escolha Permitir AWS Config para replicar dados da (s) conta (s) de origem em uma conta agregadora. Marque esta caixa de seleção para continuar adicionando um agregador.
4. Em Aggregator name (Nome do agregador), digite o nome do seu agregador.

   O nome do agregador deve ser um nome exclusivo com um máximo de 64 caracteres alfanuméricos. O nome pode conter hifens e sublinhados.
5. Em Select source accounts (Selecionar contas de origem), escolha Add individual account IDs (Adicionar IDs de contas individuais) ou Add my organization (Adicionar minha organização) para agregar dados.

   > **Note**
   >
   > A autorização é necessária ao usar Adicionar IDs de contas individuais para selecionar contas de origem.

   - Se você escolher Add individual account IDs (Adicionar IDs de contas individuais), poderá adicionar IDs de conta individuais para uma conta de agregador.

1. Escolha Add source accounts (Adicionar contas de origem) para adicionar IDs de conta.
2. Escolha Adicionar Conta da AWS IDs para adicionar manualmente IDs separadas por vírgula Conta da AWS . Se você quiser agregar dados da conta atual, digite o ID da conta.

   OU

   Escolha Carregar um arquivo para carregar um arquivo (.txt ou .csv) de IDs separados por vírgula. Conta da AWS
3. Escolha Add source accounts (Adicionar contas de origem) para confirmar sua seleção.

- Se você escolher Add my organization (Adicionar minha organização), poderá adicionar todas as contas da sua organização a uma conta agregadora.

> **Note**
>
> É necessário estar conectado à conta de gerenciamento ou à conta de gerenciamento delegado e todos os recursos devem estar habilitados em sua organização.
> Se o chamador for uma conta de gerenciamento, AWS Config chama a `EnableAwsServiceAccess` API para permitir a integração entre AWS Config e. AWS Organizations Se o chamador for um administrador delegado registrado, AWS Config chama a `ListDelegatedAdministrators` API para verificar se o chamador é um administrador delegado válido.
> Certifique-se de que a conta de gerenciamento registre o administrador delegado como nome principal do AWS Config serviço (config.amazonaws.com) antes que o administrador delegado crie um agregador. Para registrar um administrador delegado, consulte Registrar um administrador delegado.

Você deve atribuir uma função do IAM para permitir AWS Config a chamada de APIs somente de leitura para sua organização.

1. Escolha Selecione uma função de sua conta para selecionar um perfil do IAM existente.

> **Note**
>
> No console do IAM, anexe a política gerenciada pelo `AWSConfigRoleForOrganizations` ao seu perfil do IAM. Anexar essa política permite AWS Config chamar AWS Organizations `DescribeOrganization` e `ListAccounts` APIs. `ListAWSServiceAccessForOrganization` Por padrão,

`config.amazonaws.com` é automaticamente especificado como uma entidade confiável.

2. Escolha Criar uma função e digite o nome do perfil do IAM para criar um perfil do IAM.

6. Em Regions (Regiões), escolha as regiões para as quais você deseja agregar dados.
   - Selecione uma região, várias regiões ou todas as Regiões da AWS.
   - Selecione Incluir futuro Regiões da AWS para agregar dados de todos os futuros em que a agregação de dados multicontas e multirregiões Regiões da AWS está ativada.
7. Escolha Salvar. AWS Config exibe o agregador.

Editar um agregador

1. Para fazer alterações no agregador, escolha o nome dele.
2. Escolha Ações e, em seguida, Editar.
3. Use as seções na página Editar agregador para alterar as contas de origem, os perfis do IAM ou as regiões para o agregador.

> **Note**
>
> Você não pode alterar o tipo de fonte de contas individuais para organização e vice-versa.

4. Escolha Salvar.

Excluir um agregador

1. Para excluir um agregador, escolha o nome do agregador.
2. Escolha Ações e, em seguida, escolha Excluir.

   Uma mensagem de aviso é exibida. A exclusão de um agregador resultará na perda de todos os dados agregados. Você não pode recuperar esses dados, mas os dados nas contas de origem não são afetados.
3. Escolha Delete (Excluir) para confirmar sua seleção.

Configurando um agregador usando o AWS Command Line Interface

Você pode criar, visualizar, atualizar e excluir dados AWS Config agregadores usando o AWS Command Line Interface (AWS CLI).

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, insira `aws configure` para configurar o AWS CLI para usar uma AWS região em que os agregadores estejam disponíveis.

Tópicos

- Adicionar um agregador usando contas individuais
- Adicionar um agregador usando o AWS Organizations
- Registrar um administrador delegado
- Visualizar um agregador
- Editar um agregador
- Excluir um agregador

Adicionar um agregador usando contas individuais

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando a seguir para criar um agregador chamado **`MyAggregator`**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

Para `account-aggregation-sources`, insira um dos itens a seguir.

- Uma lista separada por vírgulas de Conta da AWS IDs para as quais você deseja agregar dados. Coloque os IDs da conta entre colchetes e não se esqueça de evitar aspas (por exemplo: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\", \"AccountID3\"],\"AllAwsRegions\": true}]"`).
- Você também pode fazer upload de um arquivo JSON de IDs separados por vírgula Conta da AWS . Faça upload do arquivo usando a seguinte sintaxe: `--account-aggregation-sources MyFilePath/MyFile.json`

  O arquivo JSON deve estar no seguinte formato:

```
[
    {
        "AccountIds": [
            "AccountID1",
            "AccountID2",
            "AccountID3"
        ],
        "AllAwsRegions": true
    }
]
```

3. Pressione a tecla Enter para executar o comando.

   Você deve ver saída semelhante a:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
```

```
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Adicionar um agregador usando o AWS Organizations

Antes de começar este procedimento, você precisa estar conectado à conta principal ou a um administrador delegado registrado, e todos os recursos devem estar habilitados na sua organização.

> **Note**
>
> Certifique-se de que a conta de gerenciamento registre um administrador delegado com os dois nomes principais de AWS Config serviço a seguir (`config.amazonaws.comeconfig-multiaccountsetup.amazonaws.com`) antes que o administrador delegado crie um agregador. Para registrar um administrador delegado, consulte Registrar um administrador delegado.

1. Abra um prompt de comando ou uma janela do terminal.
2. Se não tiver criado uma função do IAM para seu AWS Config agregador, insira o seguinte comando:

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> Copie o Amazon Resource Name (ARN) dessa função do IAM para uso ao criar seu AWS Config agregador. É possível encontrar o ARN no objeto de resposta.

3. Se não tiver anexado uma política à sua função do IAM, anexe a política AWSConfigRoleForOrganizationsgerenciada ou digite o seguinte comando:

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAWSSe
```

4. Digite o comando a seguir para criar um agregador chamado **MyAggregator**.

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",
\"AllAwsRegions\": true}"
```

5. Pressione a tecla Enter para executar o comando.

   Você deve ver saída semelhante a:

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Registrar um administrador delegado

Administradores delegados são contas dentro de uma determinada AWS organização que recebem privilégios administrativos adicionais para um serviço específico. AWS

1. Faça login com as credenciais da conta de gerenciamento.
2. Abra um prompt de comando ou uma janela do terminal.
3. Insira o comando a seguir para habilitar o acesso ao serviço como administrador delegado da sua organização para implantar e gerenciar AWS Config regras e pacotes de conformidade em toda a organização:

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. Insira o comando a seguir para habilitar o acesso ao serviço como administrador delegado da sua organização para agregar AWS Config dados em toda a organização:

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. Para conferir se a habilitação do acesso ao serviço foi concluída, digite o comando a seguir e pressione Enter para executar o comando.

```
aws organizations list-aws-service-access-for-organization
```

Você deve ver saída semelhante a:

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. Depois, digite o comando a seguir para registrar uma conta de membro como administrador delegado para AWS Config.

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

e

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. Para conferir se o registro do administrador delegado foi concluído, digite o comando a seguir na conta de gerenciamento e pressione Enter para executar o comando.

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

e

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

Você deve ver saída semelhante a:

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::MemberAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

Visualizar um agregador

1. Digite o comando :

```
aws configservice describe-configuration-aggregators
```

2. Dependendo da sua conta de origem, você deverá ver uma saída semelhante à seguinte:

   Para contas individuais

```
{
```

```
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

OU

Para uma organização

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Editar um agregador

1. Você pode usar o comando `put-configuration-aggregator` para atualizar ou editar um agregador de configuração.

   Digite o seguinte comando para adicionar um novo ID de conta a **`MyAggregator`**:

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
 MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

2. Dependendo da sua conta de origem, você deverá ver uma saída semelhante à seguinte:

   Para contas individuais

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

   OU

   Para uma organização

```
{
    "ConfigurationAggregator": {
```

```
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Excluir um agregador

Digite o comando :

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
 MyAggregator
```

Se for bem sucedido, o comando será executado sem saída adicional.

Autorizando contas agregadoras a coletar dados AWS Config de configuração e conformidade usando o console

AWS Config permite que você autorize contas a coletar dados AWS Config de configuração e conformidade.

Na página Authorizations (Autorizações), você pode fazer o seguinte:

- Adicionar uma autorização para permitir que uma conta de agregador e uma região coletem dados de configuração e conformidade do AWS Config .
- Autorizar uma solicitação pendente de uma conta de agregador para coletar dados de configuração e conformidade do AWS Config .
- Exclua uma autorização de uma conta agregadora para coletar dados de configuração do AWS Config e dados de conformidade da sua conta atual.

Tópicos

- Considerações
- Adicionar autorização para contas e regiões do agregador
- Autorizar uma solicitação pendente para uma conta do agregador
- Exclua uma autorização de uma conta de agregador existente

Considerações

Há dois tipos de agregadores: agregador de contas individuais e agregador organizacional

Para um agregador de contas individual, a autorização é necessária para todas as contas de origem e regiões que você deseja incluir, incluindo contas externas e regiões e contas de membros e regiões da organização.

Para um agregador de organização, a autorização não é necessária para regiões de contas de membros da organização, pois a autorização é integrada ao AWS Organizations serviço.

Os agregadores não são ativados automaticamente AWS Config em seu nome

AWS Config precisa ser habilitado na conta de origem e na região para qualquer tipo de agregador, para que AWS Config os dados sejam gerados na conta de origem e na região.

Adicionar autorização para contas e regiões do agregador

Você pode adicionar autorização para conceder permissão às contas e regiões do agregador para coletar dados de AWS Config configuração e conformidade.

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Navegue até a página Authorizations (Autorizações) e escolha Add authorization (Adicionar autorização).
3. Para Aggregator account (Conta de agregador), digite o ID de 12 dígitos da conta de agregador.
4. Para a região Agregador, escolha Regiões da AWS onde a conta do agregador tem permissão para coletar dados de configuração e conformidade AWS do Config.
5. Escolha Add authorization (Adicionar autorização) para confirmar sua seleção.

   AWS Config exibe uma conta agregadora, região e status de autorização.

> **Note**
>
> Você também pode adicionar autorizações às contas e regiões do agregador de forma programática usando AWS CloudFormation modelos de amostra. Para obter mais informações, consulte AWS::Config::AggregationAuthorizationo Guia AWS CloudFormation do usuário.

Autorizar uma solicitação pendente para uma conta do agregador

Se houver uma solicitação de autorização pendente para uma conta de agregador existente, você verá o status da solicitação na página Autorizações. Você pode autorizar uma solicitação pendente nesta página.

1. Escolha a conta agregadora que você deseja autorizar e, em seguida, escolha Autorizar.

   Uma mensagem de confirmação é exibida para confirmar que você deseja conceder permissão à conta agregadora para coletar AWS Config dados dessa conta.
2. Escolha Autorizar novamente para confirmar que você deseja conceder permissão à conta agregadora.

   O status da autorização muda de Requesting for authorization (Solicitando autorização) para Authorized (Autorizado).

Período de aprovação da autorização

A aprovação da autorização é necessária para adicionar contas de origem a um agregador de contas individual. Uma solicitação de aprovação de autorização pendente ficará disponível por sete dias após um agregador de contas individual adicionar uma conta de origem.

Exclua uma autorização de uma conta de agregador existente

1. Para a conta de agregador da qual você quer excluir a autorização, escolha Excluir.

   Uma mensagem de aviso é exibida. Quando você exclui essa autorização, AWS Config os dados não serão mais compartilhados com a conta agregadora.
2. Escolha Excluir para confirmar sua seleção.

A conta do agregador agora é excluída.

Depois que a autorização para um agregador for excluída, os dados permanecerão na conta do agregador por até 24 horas antes de serem excluídos.

Autorizando contas agregadoras a coletar dados AWS Config de configuração e conformidade usando o AWS Command Line Interface

Você pode autorizar contas agregadoras a coletar AWS Config dados das contas de origem e excluir contas agregadoras usando o AWS Command Line Interface ().AWS CLI Para usar o AWS Management Console, consulteAutorizando contas agregadoras a coletar dados AWS Config de configuração e conformidade usando o console.

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, digite `aws configure` para configurar o AWS CLI para usar uma AWS região em que os pacotes de AWS Config conformidade estejam disponíveis.

Tópicos

- Considerações
- Adicionar autorização para contas e regiões do agregador
- Excluir uma conta de autorização

Considerações

Há dois tipos de agregadores: agregador de contas individuais e agregador organizacional

Para um agregador de contas individual, a autorização é necessária para todas as contas de origem e regiões que você deseja incluir, incluindo contas externas e regiões e contas de membros e regiões da organização.

Para um agregador de organização, a autorização não é necessária para regiões de contas de membros da organização, pois a autorização é integrada ao AWS Organizations serviço.

Os agregadores não são ativados automaticamente AWS Config em seu nome

AWS Config precisa ser habilitado na conta de origem e na região para qualquer tipo de agregador, para que AWS Config os dados sejam gerados na conta de origem e na região.

Adicionar autorização para contas e regiões do agregador

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando :

```
aws configservice put-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

3. Você deve ver saída semelhante a:

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

Excluir uma conta de autorização

Digite o comando :

```
aws configservice delete-aggregation-authorization --authorized-account-id  AccountID
 --authorized-aws-region Region
```

Se for bem sucedido, o comando será executado sem saída adicional.

Consultar o estado atual da configuração dos recursos da AWS

Apresentando um recurso de visualização para consultas avançadas que permite usar recursos de inteligência artificial generativa (IA generativa) para inserir solicitações em inglês simples e convertê-las em um formato de consulta. ready-to-use Para obter mais informações, consulte Natural language query processor for advanced queries.

Você pode usar AWS Config para consultar o estado atual da configuração dos AWS recursos com base nas propriedades de configuração de uma única conta e região ou em várias contas e regiões. Você pode realizar consultas baseadas em propriedades com base nos metadados atuais do estado do AWS recurso em uma lista de recursos que oferece suporte. AWS Config Para obter mais informações sobre a lista de tipos de recursos compatíveis, consulte Supported Resource Types for Advanced Queries.

As consultas avançadas fornecem um único ponto final de consulta e uma linguagem de consulta para obter os metadados atuais do estado do recurso sem realizar chamadas de API de descrição específicas do serviço. Você pode usar agregadores de configuração para executar as mesmas consultas de uma conta central em várias contas e AWS regiões.

Tópicos

- Atributos
- Componentes da consulta
- Consultas de exemplo
- Exemplos de consultas de relacionamento
- Limitações
- Suporte regional
- Consultar usando o editor de consultas SQL (console)
- Consulta usando o Editor de consultas SQL (AWS CLI)
- Processador de consultas em linguagem natural para consultas avançadas

Atributos

AWS Config usa um subconjunto da `SELECT` sintaxe da linguagem de consulta estruturada (SQL) para realizar consultas e agregações baseadas em propriedades nos dados do item de configuração (CI) atual. As consultas variam em complexidade, desde correspondências com identificadores de tags e/ou recursos até consultas mais complexas, como a visualização de todos os buckets do Amazon S3 que têm o versionamento desativado. Isso permite que você consulte exatamente o estado atual do recurso de que você precisa sem realizar chamadas de API para serviços específicos da AWS .

Ele oferece suporte a funções de agregação, como `AVG`, `COUNT`, `MAX`, `MIN`, e `SUM`.

Você pode usar as consultas avançadas para:

- Gerenciamento de inventário, por exemplo, para recuperar uma lista de instâncias do Amazon EC2 de um determinado tamanho.
- Segurança e inteligência operacional, por exemplo, para recuperar uma lista de recursos que tenham uma propriedade de configuração específica habilitada ou desabilitada.
- Otimização de custos, por exemplo, para identificar uma lista de volumes do Amazon EBS que não estejam anexadas a nenhuma instância do EC2.
- Dados de conformidade; por exemplo, recuperar uma lista de todos os seus pacotes de conformidade e seu status de conformidade.

Para obter informações sobre como usar a linguagem de consulta AWS SQL, consulte O que é SQL (linguagem de consulta estruturada)? .

Componentes da consulta

Os componentes da consulta SQL `SELECT` são os seguintes.

Resumo

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

Parâmetros

[WHERE condição]

Filtra resultados de acordo com o `condition` especificado por você.

[propriedade GROUP BY]

Agrega o conjunto de resultados em grupos de linhas com valores correspondentes para a propriedade especificada.

A cláusula GROUP BY é aplicável às agregações.

[propriedade ORDER BY [ASC | DESC] [, propriedade [ASC | DESC] ...]]

Classifica um conjunto de resultados por um ou mais `properties` de saída.

Quando a cláusula contém várias propriedades, o conjunto de resultados é classificado de acordo com a primeira `property` e depois de acordo com a segunda `property` para as linhas que tenham valores correspondentes com os da primeira propriedade, e assim por diante.

Exemplos

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

Consultas de exemplo

Query to list all EC2 instances with AMI ID ami-12345

Consulta:

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
```

```
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

Resultados:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
```

```
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

Consulta:

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

Resultados:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

Consulta:

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

Resultados:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

Consulta:

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

Resultados:

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

Consulta:

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
```

```
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

Resultados:


```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
```

```
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Exemplos de consultas de relacionamento

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

OU

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

Limitações

> **Note**
>
> A consulta avançada não oferece suporte à consulta de recursos que não foram configurados para serem registrados pelo gravador de configuração. AWS Config cria itens de configuração (CIs) `configurationItemStatus` quando um recurso é descoberto, mas não está configurado para ser registrado pelo gravador de configuração. `ResourceNotRecorded` Embora um agregador agregue esses CIs, a consulta avançada não oferece suporte à consulta de CIs com `ResourceNotRecorded`. Atualize as configurações do gravador para permitir a gravação dos tipos de recursos que você deseja consultar.

Como um subconjunto do SQL `SELECT`, a de sintaxe de consulta tem as seguintes limitações:

- Não há suporte para as palavras-chave `ALL`, `AS`, `DISTINCT`, `FROM`, `HAVING`, `JOIN` e `UNION` em uma consulta. Não há suporte para consultas com valor `NULL`.
- Não há suporte para consultas de recursos de terceiros. Recursos de terceiros recuperados usando consultas avançadas terão o campo de configuração definido como `NULL`.
- Não há suporte para que estruturas aninhadas (como tags) sejam descompactadas com consultas SQL.
- A notação CIDR é convertida em intervalos de IP para pesquisa. Isso significa que `"="` e `"BETWEEN"` faz a pesquisa de qualquer intervalo que inclua o IP fornecido, em vez de um exato. Para pesquisar um intervalo de IP exato, você precisa inserir condições adicionais para excluir IPs fora do intervalo. Por exemplo, para pesquisar 10.0.0.0/24 e somente esse bloco de IP, você pode fazer:

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
```

```
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Para 192.168.0.2/32, você pode pesquisar de forma semelhante:

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

- Ao consultar em relação a várias propriedades dentro de uma matriz de objetos, as correspondências são calculadas em relação a todos os elementos da matriz. Por exemplo, para um recurso R com as regras A e B, o recurso está em conformidade com a regra A, mas não está em conformidade com a regra B. O recurso R é armazenado como:

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

R será retornado por esta consulta:

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

A primeira condição `configuration.configRuleList.complianceType = 'non_compliant'` é aplicada a TODOS os elementos em R.configRuleList, porque R tem uma regra (regra B) com complianceType = 'non_compliant', a condição é avaliada como verdadeira. A segunda condição `configuration.configRuleList.configRuleName` é aplicada a TODOS

os elementos em R.configRuleList, porque R tem uma regra (regra A) com configRuleName = 'A', a condição é avaliada como verdadeira. Como ambas as condições são verdadeiras, R será retornado.

- A abreviação `SELECT` de todas as colunas (ou seja, `SELECT *`) seleciona somente propriedades escalares de nível superior de um CI. As propriedades escalares retornadas são `accountId`, `awsRegion`, `arn`, `availabilityZone`, `configurationItemCaptureTime`, `resourceCreationTime`, `resourceId`, `resourceName`, `resourceType`, e `version`.
- Limitações curinga:
  - Curingas têm suporte somente para valores de propriedade e não para chaves de propriedade (por exemplo, `...WHERE someKey LIKE 'someValue%'` tem suporte, mas `...WHERE 'someKey%' LIKE 'someValue%'` não).
  - Suporte somente para sufixos curingas (por exemplo, `...LIKE 'AWS::EC2::%'` e `...LIKE 'AWS::EC2::_'` tem suporte, mas `...LIKE '%::EC2::Instance'` e `...LIKE '_::EC2::Instance'` não).
  - As correspondências que envolvem curingas devem ter pelo menos três caracteres (por exemplo, `...LIKE 'ab%'` e `...LIKE 'ab_'` não é permitido, mas `...LIKE 'abc%'` e `...LIKE 'abc_'` é permitido).

> **Note**
>
> O "_" (sublinhado único) também é tratado como um curinga.

- Limitações de agregação:
  - As funções agregadas podem aceitar somente um único argumento ou propriedade.
  - As funções agregadas não podem tomar outras funções como argumentos.
  - `GROUP BY` com uma cláusula `ORDER BY` que faz referência às funções agregadas pode conter somente uma única propriedade.
  - Para todas as outras agregações, as cláusulas `GROUP BY` podem conter até três propriedades.
  - A paginação é compatível com todas as consultas agregadas, exceto quando a cláusula `ORDER BY` tem uma função agregada. Por exemplo, `GROUP BY X, ORDER BY Y` não funciona se Y for uma função agregada.
  - Não há suporte para cláusulas `HAVING` nas agregações.
- Limitações de identificadores incompatíveis:

Identificadores incompatíveis são propriedades que têm a mesma grafia, mas com capitalização diferente (letras maiúsculas e minúsculas). A consulta avançada não oferece suporte ao processamento de consultas que contêm identificadores incompatíveis. Por exemplo: .

- Duas propriedades que têm exatamente a mesma grafia, mas com letras maiúsculas e minúsculas diferentes (`configuration.dbclusterIdentifier` e `configuration.dBClusterIdentifier`).
- Duas propriedades em que uma propriedade é um subconjunto da outra e elas têm letras maiúsculas e minúsculas diferentes (`configuration.ipAddress` e `configuration.ipaddressPermissions`).

Suporte regional

As consultas avançadas têm suporte nas seguintes regiões:

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (Norte da Califórnia)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
África (Cidade do Cabo)	af-south-1	config.af-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hong Kong)	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Ásia-Pacífico (Hyderabad)	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
Ásia-Pacífico (Jacarta)	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Melbourne)	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
Ásia-Pacífico (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Ásia-Pacífico (Osaka)	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Ásia-Pacífico (Seul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Ásia-Pacífico (Singapura)	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Ásia-Pacífico (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Ásia-Pacífico (Tóquio)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canadá (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
Oeste do Canadá (Calgary)	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
Europa (Frankfurt)	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
Europa (Milão)	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
Europa (Paris)	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo
Europa (Espanha)	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
Europa (Zurique)	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	config.il-central-1.amazonaws.com	HTTPS
Oriente Médio (Barém)	me-south-1	config.me-south-1.amazonaws.com	HTTPS
Oriente Médio (Emirados Árabes Unidos)	me-central-1	config.me-central-1.amazonaws.com	HTTPS
América do Sul (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Leste dos EUA)	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS

Nome da região	Região	Endpoint	Protocolo	
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS	

Consultar usando o editor de consultas SQL (console)

Apresentando um recurso de visualização para consultas avançadas que permite usar recursos de inteligência artificial generativa (IA generativa) para inserir solicitações em inglês simples e convertê-las em um formato de consulta. ready-to-use Para obter mais informações, consulte Natural language query processor for advanced queries.

Você pode usar consultas de AWS amostra ou criar sua própria consulta, chamada de consultas personalizadas.

Considerações

Pré-requisitos

Se você estiver usando uma das seguintes políticas AWS gerenciadas, terá as permissões necessárias para executar e salvar uma consulta: AWSServiceRoleForConfig(função vinculada ao serviço) ou AWS_. ConfigRole

Caso contrário, você deverá ter as permissões incluídas na política AWSConfigUserAccess AWS gerenciada.

Lista de propriedades que você pode consultar

Uma lista atualizada de propriedades e seus tipos de dados está disponível em GitHub.

Consultas e agregadores avançados

Para executar uma consulta em um agregador, crie um agregador. Para ter mais informações, consulte Configurar um agregador usando o console.

Se você já tiver um agregador configurado, no escopo da consulta, escolha-o para executar uma consulta avançada nesse agregador. Ao selecionar um agregador, considere adicionar o Conta da AWS ID e a AWS região na instrução de consulta para visualizar essas informações nos resultados.

Use uma consulta AWS de amostra

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Escolha Advanced queries (Consultas avançadas) na navegação à esquerda para consultar as configurações de recursos de uma única conta e região ou de várias contas e regiões.
3. Na página Consultas avançadas, escolha uma consulta apropriada na lista de consultas. É possível filtrar a lista de consultas por nome, descrição, criador ou tags. Para filtrar consultas da AWS , selecione Criar e digite AWS. A consulta selecionada é exibida no editor de consultas SQL. É possível editar a consulta selecionada para atender às necessidades.
4. Para salvar essa consulta em uma nova consulta, escolha Salvar como.
   - No campo Nome da consulta, atualize o nome da consulta.
   - No campo Descrição, atualize a descrição da consulta.
   - Insira até 50 tags exclusivas para essa consulta.
   - Escolha Salvar.
5. Escolha Executar. Os resultados da consulta serão exibidos na tabela abaixo do editor de consultas.
6. Escolha Export as (Exportar como) para exportar os resultados da consulta no formato CSV ou JSON.

> **Note**
>
> Os resultados da consulta são paginados. Até quinhentos resultados são exportados. Também é possível usar as APIs para recuperar todos os resultados. Os resultados são paginados e você pode recuperar 100 resultados por vez.

Crie sua consulta personalizada

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.

2. Escolha Advanced queries (Consultas avançadas) na navegação à esquerda para consultar as configurações de recursos de uma única conta e região ou de várias contas e regiões.
3. Para criar sua consulta personalizada, escolha Nova consulta.

   Para visualizar ou editar uma consulta personalizada, filtre uma consulta por nome, descrição, criador ou tags. Para filtrar consultas personalizadas, escolha Criador e insira Personalizado.
4. Na página Editor de consultas, em Nova consulta, crie sua própria consulta para essa conta e região. Também é possível selecionar um agregador apropriado a fim de criar uma consulta para várias contas e regiões.
5. Edite, se quiser fazer alterações nessa consulta. Para salvar essa consulta, escolha Salvar.
   - No campo Nome da consulta, atualize o nome da consulta.
   - No campo Descrição, atualize a descrição da consulta.
   - Insira até 50 tags exclusivas para essa consulta.
   - Escolha Salvar.
6. Escolha Executar. Os resultados da consulta serão exibidos na tabela abaixo do editor de consultas.
7. Escolha Export as (Exportar como) para exportar os resultados da consulta no formato CSV ou JSON.

   Os resultados da consulta são paginados. Até quinhentos resultados são exportados.

   Também é possível usar as APIs para recuperar todos os resultados. Os resultados são paginados e você pode recuperar 100 resultados por vez.

Consulta usando o Editor de consultas SQL (AWS CLI)

AWS CLI É uma ferramenta unificada para gerenciar seus AWS serviços. Com apenas uma ferramenta para baixar e configurar, você pode controlar vários AWS serviços na linha de comando e usar scripts para automatizá-los. Para obter mais informações sobre o AWS CLI e para obter instruções sobre como instalar as AWS CLI ferramentas, consulte o seguinte no Guia AWS Command Line Interface do usuário.

- AWS Command Line Interface Guia do usuário
- Começando com AWS Command Line Interface

Se necessário, insira `aws configure` para configurar o AWS CLI para usar uma AWS região em que consultas avançadas estejam disponíveis.

Considerações

Pré-requisitos

Se você estiver usando uma das seguintes políticas AWS gerenciadas, terá as permissões necessárias para executar e salvar uma consulta: AWSServiceRoleForConfig(função vinculada ao serviço) ou AWS_. ConfigRole

Caso contrário, você deverá ter as permissões incluídas na política AWSConfigUserAccess AWS gerenciada.

Lista de propriedades que você pode consultar

Uma lista atualizada de propriedades e seus tipos de dados está disponível em GitHub.

Consultas e agregadores avançados

Para executar uma consulta em um agregador, crie um agregador. Para ter mais informações, consulte Configurar um agregador usando o console.

Se você já tiver um agregador configurado, no escopo da consulta, escolha-o para executar uma consulta avançada nesse agregador. Ao selecionar um agregador, considere adicionar o Conta da AWS ID e a AWS região na instrução de consulta para visualizar essas informações nos resultados.

Dados de configuração do recurso de consulta

Como consultar os dados de configuração de recursos usando o editor de consultas (AWS CLI) para uma única conta e região

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando a seguir para consultar os dados de configuração do recurso.

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

Dependendo da consulta, a saída será semelhante à seguinte:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

Como consultar os dados de configuração de recursos usando o editor de consultas (AWS CLI) para várias contas e regiões

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando a seguir para consultar os dados de configuração do recurso.

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

Dependendo da consulta, a saída será semelhante à seguinte:

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
```

```
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> Ao usar os tipos de `AWS::IAM::Policy` recursos `AWS::IAM::User` `AWS::IAM::GroupAWS::IAM::Role`,, e em uma consulta avançada, use`awsRegion = 'global'`.

Salvar uma consulta

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando a seguir para salvar uma consulta.

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. Dependendo da consulta, a saída será semelhante à seguinte:

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` é opcional. Quando você passa as tags, as tags salvas não serão retornadas por `list-stored-queries` ou `get-stored-query`. Você deve usar `list-tag-for-resources` para recuperar as tags associadas a uma consulta salva.

`--description` é opcional ao criar ou atualizar uma consulta.

Exibir todas as consultas salvas

1. Digite o comando a seguir para ver a lista de todas as consultas salvas.

```
aws configservice list-stored-queries
```

2. Dependendo da consulta, a saída será semelhante à seguinte:

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

Obter detalhes de uma consulta salva

1. Digite o comando a seguir para obter detalhes de uma consulta salva específica.

```
aws configservice get-stored-query --query-name cli-test
```

2. Dependendo da consulta, a saída será semelhante à seguinte:

```
{
    "StoredQuery": {
```

```
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

Excluir uma consulta salva

- Digite o comando a seguir para excluir sua consulta salva.

```
aws configservice delete-stored-query --query-name cli-test
```

Se for bem sucedido, o comando será executado sem saída adicional.

Processador de consultas em linguagem natural para consultas avançadas

> O processador de consulta de linguagem natural para consultas avançadas está na versão prévia AWS Config e está sujeito a alterações.

O processador de consultas em linguagem natural para consultas avançadas usa o Amazon Bedrock, uma tecnologia de inteligência artificial generativa (IA generativa) que permite inserir solicitações em inglês simples e convertê-las em um formato de consulta. ready-to-use Com o processador de consulta de linguagem natural, você pode consultar sua organização Conta da AWS ou em toda a AWS organização.

Uma solicitação pode ser uma pergunta ou uma declaração. Por exemplo, você pode inserir solicitações como “Quais balanceadores de carga são criados após 1º de janeiro de 2024?” e “Liste toda a minha função lambda que está executando o node js 16.”

Considerações

O processador de consulta de linguagem natural não pode realizar as seguintes ações:

- Gere consultas de outros idiomas além do inglês.
- Gere consultas a partir de prompts que não estão relacionados a consultas avançadas.
- Gere consultas a partir de prompts com mais de 1000 caracteres.
- Gere consultas a partir de correções de acompanhamento ou de sessões anteriores.
- Explique o código que foi gerado.

Consultar usando o processador de consultas em linguagem natural

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Escolha Advanced queries (Consultas avançadas) na navegação à esquerda para consultar as configurações de recursos de uma única conta e região ou de várias contas e regiões.
3. Na página Consultas avançadas, selecione Nova consulta para acessar o Editor de consultas.
   - (Opcional) Para executar uma consulta em um agregador, crie um agregador. Para ter mais informações, consulte Configurar um agregador usando o console.
   - Se você já tiver um agregador configurado, no escopo da consulta, selecione-o para realizar uma consulta avançada nesse agregador. Ao selecionar um agregador, considere adicionar o Conta da AWS ID e a AWS região na instrução de consulta para visualizar essas informações nos resultados.
4. No Editor de consultas, acesse a seção Processador de consultas em linguagem natural. Insira um prompt em inglês simples e escolha Gerar. Para ver exemplos, consulte Exemplos de solicitações.
5. Depois de gerar uma consulta, é possível selecionar Copiar (funcionalmente equivalente a Ctrl+C) para copiar a consulta para a área de transferência ou escolher Preencher para o editor. Se preenchida para o editor, será possível editar a consulta gerada de acordo com as necessidades.
6. Para salvar essa consulta em uma nova consulta, escolha Salvar como.
   - No campo Nome da consulta, atualize o nome da consulta.
   - No campo Descrição, atualize a descrição da consulta.
   - Insira até 50 tags exclusivas para essa consulta.
   - Escolha Salvar.

7. Escolha Executar. Os resultados da consulta serão exibidos na tabela abaixo do editor de consultas.
8. Escolha Export as (Exportar como) para exportar os resultados da consulta no formato CSV ou JSON.

> **Note**
>
> Os resultados da consulta são paginados. Até quinhentos resultados são exportados. Também é possível usar as APIs para recuperar todos os resultados. Os resultados são paginados e você pode recuperar 100 resultados por vez.

Exemplos de solicitações

A seguir estão os prompts e as consultas geradas que você pode usar como exemplos.

Example: Quais balanceadores de carga foram criados após 1º de janeiro de 2024?

Aviso: What load balancers were created after January 1, 2024?

Consulta gerada:

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: Quais das minhas instâncias de banco de dados do RDS estão acessíveis publicamente?

Aviso: Which of my RDS database instances are publicly accessible?

Consulta gerada:

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: Quantas instâncias do EC2 foram criadas no último ano?

Aviso: How many EC2 instances were created in last one year?

Consulta gerada:

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: Quantas instâncias do EC2 eu tenho em cada uma das minhas? Contas da AWS

Aviso: How many EC2 instances do I have in each of my Contas da AWS?

Consulta gerada:

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: Quais funções do IAM têm a política AdministratorAccess gerenciada anexada?

Aviso: Which IAM roles have the managed policy AdministratorAccess attached?

Consulta gerada:

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: Volumes do EBS sem criptografia

Aviso: EBS volumes without encryption

Consulta gerada:

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: Obtenha recursos não compatíveis

Aviso: Get noncompliant resources

Consulta gerada:

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: Listar toda a minha função lambda que está executando o node js 16

Aviso: List all my lambda function that is running node js 16

Consulta gerada:

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: Quais certificados do ACM expirarão nos próximos 30 dias?

Aviso: What ACM certificates expire the next 30 days?

Consulta gerada:

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> Os horários na consulta gerada dependem do horário em que você insere o prompt.

Fornecer feedback

Você pode fornecer feedback geral sobre o processador de consultas de linguagem natural ou sobre uma consulta gerada específica.

Fornecendo feedback sobre o processador de consulta de linguagem natural

Escolha o botão Fornecer feedback que aparece acima do processador de consultas de linguagem natural à direita. Você pode inserir sua satisfação ou insatisfação e fornecer feedback sobre como AWS Config tornar a consulta em linguagem natural mais útil.

> **Note**
>
> Não divulgue nenhuma informação pessoal, comercialmente sensível ou confidencial.

Fornecendo feedback sobre uma consulta gerada específica

Você pode fornecer seu feedback sobre uma consulta gerada escolhendo o botão de polegar para cima ou para baixo que aparece abaixo da consulta gerada.

Suporte regional

O processador de consultas em linguagem natural é compatível nas regiões a seguir.

Nome da região	Região	Endpoint	Protocolo
Leste dos EUA (Norte da Virgínia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
Oeste dos EUA (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Excluindo dados AWS Config

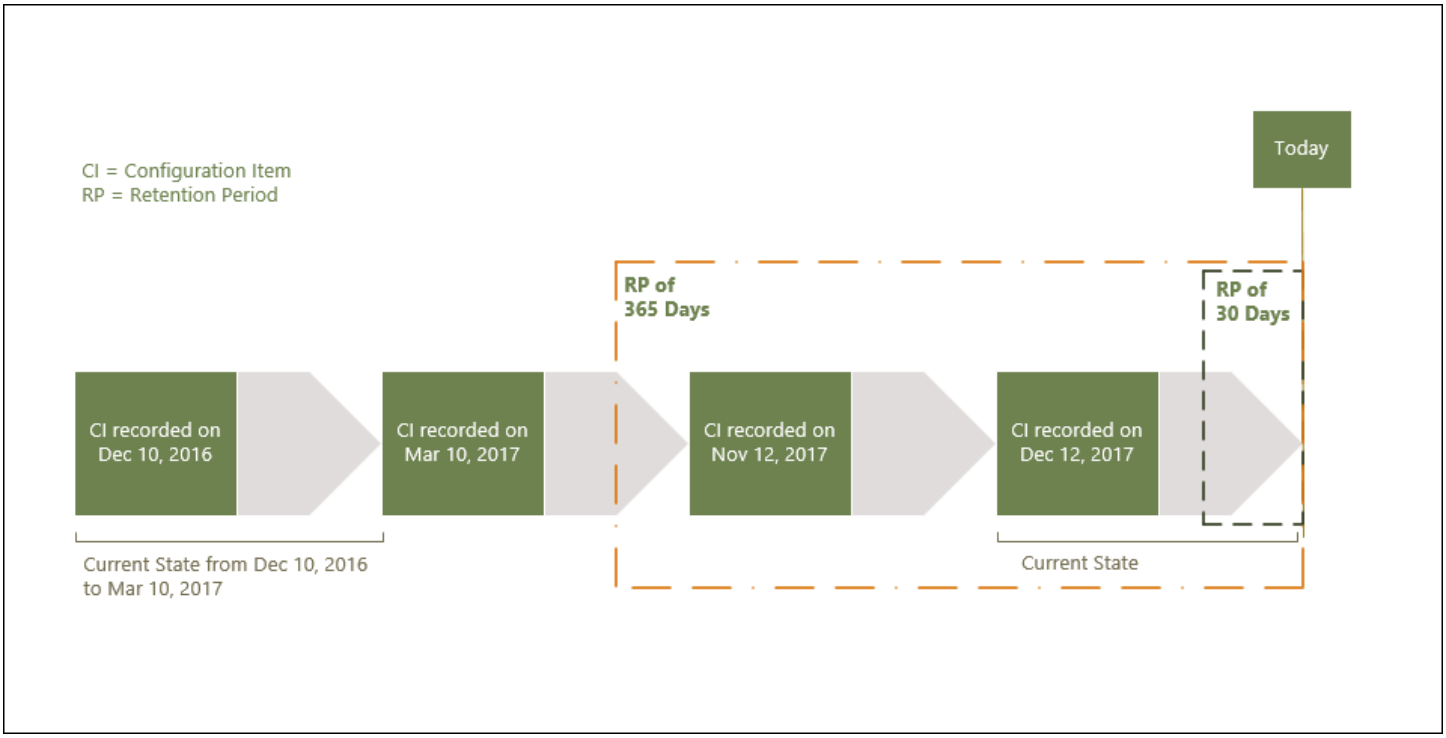
> **Note**
>
> AWS Config A While usa o Amazon Simple Storage Service (Amazon S3) e o Amazon Simple Notification Service (Amazon SNS) para enviar snapshots de configuração e arquivos de AWS Config histórico de configuração, tem seu próprio armazenamento de dados e políticas de retenção. As informações nesta página são específicas para AWS Config. O Amazon S3 e o Amazon SNS têm suas próprias políticas separadas de armazenamento e retenção de dados.

AWS Config permite que você exclua seus dados especificando um período de retenção para seus`ConfigurationItems`. Quando você especifica um período de retenção, AWS Config retém o seu `ConfigurationItems` por esse período especificado. Você pode escolher um período entre um mínimo de 30 dias e um máximo de 7 anos (2557 dias). AWS Config exclui dados anteriores ao período de retenção especificado. Se você não especificar um período de retenção, o AWS Config continuará armazenando `ConfigurationItems` pelo período padrão de 7 anos (2.557 dias). Quando a gravação está ativada, o estado atual do recurso é quando um `ConfigurationItem` é registrado e até a próxima alteração (um novo `ConfigurationItem`) ser registrada.

Para compreender o comportamento do período de retenção, vamos dar uma olhada no cronograma.

- Quando a gravação está ativada, o estado atual de um recurso sempre existe e não pode ser excluído independentemente da data em que o `ConfigurationItem` é registrado.
- Quando AWS Config os registros são novos`ConfigurationItems`, os anteriores `ConfigurationItems` são excluídos dependendo do período de retenção especificado.

Na linha do tempo a seguir, AWS Config registros `ConfigurationItems` nas seguintes datas. Para os fins deste cronograma, hoje é representado como 24 de maio de 2018.



A tabela a seguir explica que `ConfigurationItems` são exibidos no cronograma do AWS Config com base no período de retenção selecionado.

Período de retenção	Itens de configuração exibidos no cronograma	Explicação
30 dias	12 de dezembro de 2017	O estado atual do recurso iniciado em 12 de dezembro de 2017 quando o `ConfigurationItem` foi registrado e é válido até hoje (24 de maio de 2018). Quando a gravação está ativada, o estado atual sempre existe.
365 dias	12 de dezembro de 2017; 12 de novembro de 2017 e 10 de março de 2017	O período de retenção mostra o estado atual de 12 de dezembro de 2017 e os `ConfigurationItems` anteriores de 12 de novembro de 2017 e 10 de março de 2017.

Período de retenção	Itens de configuração exibidos no cronograma	Explicação
		O `ConfigurationItem` de 10 de março de 2017 é exibido no cronograma, pois esse estado de configuração representa o estado atual há 365 dias.

Depois de especificar um período de retenção, as AWS Config APIs `ConfigurationItems` que representam um estado anterior ao período de retenção especificado não são mais retornadas.

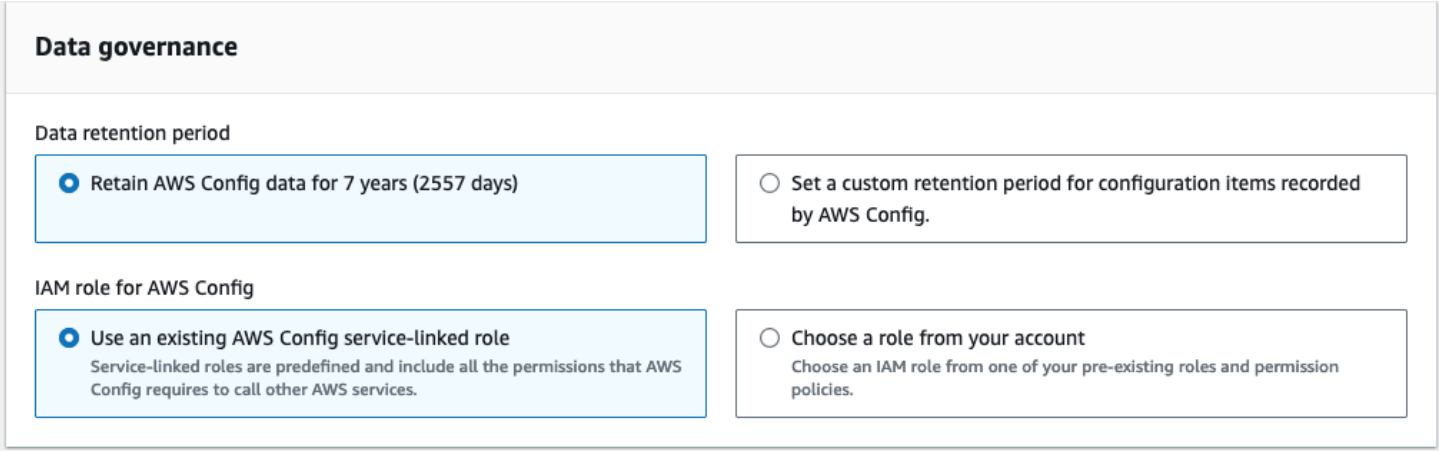
> **Note**
>
> - AWS Config não pode gravar seu `ConfigurationItems` se a gravação estiver desligada.
> - AWS Config não poderá registrá-lo `ConfigurationItems` se sua função do IAM tiver permissões insuficientes. Para obter mais informações, consulte Permissões para a função do IAM atribuída AWS Config a.

Definindo o período de retenção de dados em AWS Management Console

No AWS Management Console, se você não selecionar um período de retenção de dados, o período padrão será de 7 anos ou 2557 dias.

Para definir um período de retenção de dados personalizado para itens de configuração, marque a caixa de seleção. É possível selecionar 1 ano, 3 anos, 5 anos ou um período personalizado. Para um período personalizado, insira o número de dias entre 30 e 2557 dias.

A imagem a seguir mostra onde você pode definir o período de retenção de dados na Governança de dados. Você pode acessar a Governança de dados na página Editar configurações do AWS Config console escolhendo Configurações na barra de navegação esquerda e, em seguida, escolhendo Editar.


Data governance
Data retention period
Retain AWS Config data for 7 years (2557 days)
Set a custom retention period for configuration items recorded by AWS Config.
IAM role for AWS Config
Use an existing AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.
Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Segurança em AWS Config

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS Config, consulte os AWS serviços em Escopo por Programa AWS de Conformidade .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Config. Os tópicos a seguir mostram como configurar para atender AWS Config aos seus objetivos de segurança e conformidade.

Tópicos

- Proteção de dados em AWS Config
- Identity and Access Management para AWS Config
- Resposta a incidentes em AWS Config
- Validação de conformidade para AWS Config
- Resiliência em AWS Config
- Segurança de infraestrutura em AWS Config
- Prevenção contra o ataque do “substituto confuso” em todos os serviços
- Melhores práticas de segurança para AWS Config

Proteção de dados em AWS Config

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no AWS Config. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS LGPD e Modelo de Responsabilidade Compartilhada no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AWS Config ou outro Serviços da AWS usando o console, a API ou AWS os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de

diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados em repouso

Os dados são criptografados em repouso usando criptografia transparente do lado do servidor. Isso ajuda a reduzir a carga e a complexidade operacionais necessárias para proteger dados confidenciais. Com a criptografia de dados em repouso, você pode criar aplicativos confidenciais que atendem a requisitos de conformidade e regulamentação de criptografia.

Criptografia de dados em trânsito

Os dados coletados e acessados por nós AWS Config são exclusivamente por meio de um canal protegido pelo Transport Layer Security (TLS).

Identity and Access Management para AWS Config

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Config os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como AWS Config funciona com o IAM
- Exemplos de políticas baseadas em identidade para AWS Config
- AWS políticas gerenciadas para AWS Config
- Permissões para a função do IAM atribuída a AWS Config
- Atualização da função do IAM atribuída a AWS Config
- Permissões para o bucket Amazon S3 para o AWS Config canal de entrega
- Permissões para a chave KMS para o canal AWS Config de entrega

- Permissões para o tópico do Amazon SNS
- Solução de problemas AWS Config de identidade e acesso
- Usando funções vinculadas ao serviço para AWS Config

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS Config.

Usuário do serviço — Se você usar o AWS Config serviço para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AWS Config recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no AWS Config, consulte Solução de problemas AWS Config de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AWS Config recursos da sua empresa, provavelmente tem acesso total AWS Config a. É seu trabalho determinar quais AWS Config recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS Config, consulteComo AWS Config funciona com o IAM.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS Config. Para ver exemplos de políticas AWS Config baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para AWS Config

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já

configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Utilizar a autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade.

Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte "O que é o Centro de Identidade do IAM?" no Guia do usuário AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de permissões no Guia do usuário AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de

serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte How SCPs work (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS Config funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AWS Config, saiba com quais recursos do IAM estão disponíveis para uso AWS Config.

Recursos do IAM que você pode usar com AWS Config

Atributo do IAM	AWS Config apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Sim
Sessões de acesso direto (FAS)	Sim
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para ter uma visão de alto nível de como AWS Config e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AWS Config

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AWS Config

Para ver exemplos de políticas AWS Config baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Config

Políticas baseadas em recursos dentro AWS Config

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para

o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AWS Config

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AWS Config ações, consulte Ações definidas por AWS Config na Referência de Autorização de Serviço.

As ações de política AWS Config usam o seguinte prefixo antes da ação:

```
config
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "config:action1",
      "config:action2"
         ]
```

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "config:Describe*"
```

Para ver exemplos de políticas AWS Config baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Config

Recursos políticos para AWS Config

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de AWS Config recursos e seus ARNs, consulte Recursos definidos por AWS Config na Referência de Autorização de Serviço. Para saber com quais ações é possível especificar o ARN de cada atributo, consulte Ações definidas pelo AWS Config.

Para ver exemplos de políticas AWS Config baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Config

Chaves de condição de política para AWS Config

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de AWS Config condição, consulte Chaves de condição AWS Config na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS Config.

Para ver exemplos de políticas AWS Config baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para AWS Config

ACLs em AWS Config

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AWS Config

Oferece compatibilidade com ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do Usuário do IAM.

Para obter mais informações sobre recursos de marcação do AWS Config , consulte Marcar os recursos do AWS Config.

Usando credenciais temporárias com AWS Config

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS "Trabalhe com o IAM" no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Sessões de acesso direto para AWS Config

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída.

Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhamento de sessões de acesso.

Funções de serviço para AWS Config

Oferece compatibilidade com funções de serviço	Sim

O perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AWS Config a funcionalidade. Edite as funções de serviço somente quando AWS Config fornecer orientação para fazer isso.

Funções vinculadas a serviços para AWS Config

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções AWS Config vinculadas a serviços, consulte. Usando funções vinculadas ao serviço para AWS Config

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna

Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para AWS Config

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do AWS Config . Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AWS Config, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS Config na Referência de Autorização de Serviço.

Tópicos

- Melhores práticas de política
- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- Usar o console do AWS Config
- Permitir que usuários visualizem suas próprias permissões
- Acesso somente para leitura a AWS Config
- Acesso total ao AWS Config
- Permissões em nível de recurso suportadas para AWS Config ações da API Rule
- Permissões no nível do recurso compatível para agregação de dados de várias contas e regiões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AWS Config recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas

AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.

- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use o URL de login que foi enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Usar o console do AWS Config

Para acessar o AWS Config console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Config recursos em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o AWS Config console, anexe também a política AWS Config `AWSConfigUserAccess` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionando Permissões a um Usuário no Guia do Usuário do IAM.

Você deve dar aos usuários permissões para interagir com AWS Config. Para usuários que precisam de acesso total AWS Config, use a política de acesso total ao AWS Config gerenciado.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acesso somente para leitura a AWS Config

O exemplo a seguir mostra uma política AWS gerenciada `AWSConfigUserAccess` que concede acesso somente para leitura a. AWS Config

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
```

```
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

Nas declarações da política, o elemento `Effect` especifica se as ações são permitidas ou negadas. O elemento `Action` lista as ações específicas que o usuário tem permissão para realizar. O elemento `Resource` lista os recursos da AWS nos quais o usuário tem permissão para realizar essas ações. Para políticas que controlam o acesso às AWS Config ações, o `Resource` elemento é sempre definido como`*`, um curinga que significa “todos os recursos”.

Os valores no elemento `Action` correspondem às APIs às quais os serviços oferecem suporte. As ações são precedidas por `config:` para indicar que se referem a ações do AWS Config . Você pode usar o caractere curinga `*` no elemento `Action`, como nos exemplos a seguir:

- `"Action": ["config:*ConfigurationRecorder"]`

  Isso permite todas as AWS Config ações que terminam com ConfigurationRecorder "" (`StartConfigurationRecorder`,`StopConfigurationRecorder`).
- `"Action": ["config:*"]`

  Isso permite todas as AWS Config ações, mas não ações para outros AWS serviços.
- `"Action": ["*"]`

  Isso permite todas as AWS ações. Essa permissão é adequada para um usuário que atua como AWS administrador da sua conta.

A política somente leitura não concede permissão de usuário a ações como `StartConfigurationRecorder`, `StopConfigurationRecorder` e `DeleteConfigurationRecorder`. Os usuários com essa política não têm permissão para iniciar,

interromper ou excluir o gravador de configuração. Para ver a lista de AWS Config ações, consulte a Referência AWS Config da API.

Acesso total ao AWS Config

O exemplo a seguir mostra uma política que concede acesso total AWS Config a. Ele concede aos usuários a permissão para realizar todas as AWS Config ações. Ela também permite que os usuários gerenciem arquivos em buckets do S3 e os tópicos do SNS na conta à qual o usuário está associado.

> **Important**
>
> Essa política concede amplas permissões. Antes de conceder acesso total, comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Essa é uma prática mais recomendada do que começar com permissões que são muito permissivas e tentar restringi-las posteriormente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
```

```
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Permissões em nível de recurso suportadas para AWS Config ações da API Rule

As permissões em nível de recurso se referem à capacidade de especificar em quais recursos os usuários podem realizar ações. AWS Config oferece suporte a permissões em nível de recurso para determinadas ações da API de AWS Config regras. Isso significa que, para determinadas ações de AWS Config regras, você pode controlar as condições sob as quais os usuários podem usar essas ações. Essas condições podem ser ações que precisam ser concluídas ou recursos específicos que os usuários têm permissão para usar.

A tabela a seguir descreve as ações da API de AWS Config regras que atualmente oferecem suporte a permissões em nível de recurso. Ela também descreve os recursos compatíveis e seus ARNs para cada ação. Ao especificar um ARN, você pode usar o caractere curinga * em seus caminhos. Por exemplo, quando você não pode ou não deseja especificar IDs exatos de recursos.

> **Important**
>
> Se uma ação de API de AWS Config regra não estiver listada nessa tabela, ela não é compatível com permissões em nível de recurso. Se uma ação de AWS Config regra não oferecer suporte a permissões em nível de recurso, você poderá conceder aos usuários permissões para usar a ação, mas precisará especificar um * para o elemento de recurso da sua declaração de política.

Ação API	Recursos
DeleteConfigRegra	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluationResultados	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeCompliance ByConfigRegra	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluatio nStatus	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfi gRule	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfigRegra	Regra do Config arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Regra do Config

Ação API	Recursos
	arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediationConfigurações	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*
DescribeRemediationConfigurações	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*
DeleteRemediationConfiguração	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*
PutRemediationExceções	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*
DescribeRemediationExceções	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*
DeleteRemediationExceções	Configuração de correção arn:aws:config:*region:accountId* :remediation-configuration/*nome da regra de configuração/Id da configuração de correção*

Por exemplo, você deseja permitir acesso de leitura e negar acesso de gravação para regras específicas a determinados usuários.

Na primeira política, você permite que a AWS Config regra leia ações como `DescribeConfigRuleEvaluationStatus` nas regras especificadas.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

Na segunda política, você nega que a AWS Config regra escreva ações na regra específica.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
```

```
    }
```

Com permissões em nível de recurso, você pode permitir o acesso de leitura e negar o acesso de gravação para realizar ações específicas nas ações da API de AWS Config regras.

Permissões no nível do recurso compatível para agregação de dados de várias contas e regiões

Você pode usar permissões no nível do recurso para controlar a capacidade do usuário de realizar ações específicas de agregação de dados em várias contas e várias regiões. As seguintes AWS Config `Aggregator` APIs oferecem suporte a permissões em nível de recurso:

- BatchGetAggregateResourceConfig
- DeleteConfigurationAgregador
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRegra
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceConta
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAgregador
- SelectAggregateResourceConfig

Por exemplo, você pode restringir o acesso aos dados de recursos para usuários específicos criando dois agregadores, `AccessibleAggregator` e `InAccessibleAggregator`, e anexando uma política do IAM que permita o acesso a `AccessibleAggregator`, mas negue o acesso a `InAccessibleAggregator`.

Política do IAM para AccessibleAggregator

Nessa política, você permite o acesso às ações agregadoras compatíveis com o nome do recurso da Amazon (ARN) do AWS Config especificado. Neste exemplo, o AWS Config ARN

é. `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

Política do IAM para InAccessibleAggregator

Nessa política, você nega acesso às ações agregadoras suportadas para o AWS Config ARN que você especifica. Neste exemplo, o AWS Config ARN é. `arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
```

```
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Se um usuário do grupo de desenvolvedores tentar realizar qualquer uma dessas ações no AWS Config ARN que você especificou, esse usuário receberá uma exceção de acesso negado.

Verificar as permissões de acesso do usuário

Para mostrar os agregadores que você criou, execute o seguinte AWS CLI comando:

```
aws configservice describe-configuration-aggregators
```

Quando o comando for concluído com sucesso, você poderá ver os detalhes de todos os agregadores associados à sua conta. Neste exemplo, eles são `AccessibleAggregator` e `InAccessibleAggregator`:

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
```

```
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> Para `account-aggregation-sources`, insira uma lista separada por vírgulas dos IDs de conta da AWS para os quais você deseja agregar dados. Coloque os IDs da conta entre colchetes e não se esqueça de evitar aspas (por exemplo: `"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`).

Anexe a seguinte política do IAM para negar o acesso a `InAccessibleAggregator` ou ao agregador ao qual você deseja negar o acesso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

Em seguida, confirme que a política do IAM funciona para restringir o acesso a regras para um agregador específico:

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

O comando deve retornar uma exceção de acesso negado:

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS políticas gerenciadas para AWS Config

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

AWS política gerenciada: AWSConfigServiceRolePolicy

AWS Config usa a função vinculada ao serviço nomeada AWSServiceRoleForConfigpara chamar outros AWS serviços em seu nome. Quando você usa o AWS Management Console para configurar AWS Config, essa SLR é criada automaticamente AWS Config se você selecionar a opção de usar a AWS Config SLR em vez de sua própria função de serviço AWS Identity and Access Management (IAM).

O SLR AWSServiceRoleForConfig contém a política gerenciada `AWSConfigServiceRolePolicy`. Essa política gerenciada contém permissões somente leitura e somente gravação para recursos e permissões somente leitura para AWS Config recursos em outros serviços que oferecem suporte. AWS Config Para obter mais informações, consulte Tipos de recursos compatíveis e Usando funções vinculadas ao serviço para AWS Config.

Veja a política: AWSConfigServiceRolePolicy.

AWS política gerenciada: AWS_ConfigRole

Para registrar suas configurações AWS de recursos, AWS Config são necessárias permissões do IAM para obter os detalhes de configuração sobre seus recursos. Se você deseja criar um perfil do

IAM para o AWS Config, use a política gerenciada `AWS_ConfigRole` e anexe-a ao seu perfil do IAM.

Essa política do IAM é atualizada sempre que AWS Config adiciona suporte para um tipo de AWS recurso. Isso significa que AWS Config continuará a ter as permissões necessárias para registrar dados de configuração dos tipos de recursos suportados, desde que a ConfigRole função AWS_ tenha essa política gerenciada anexada. Para obter mais informações, consulte Tipos de recursos compatíveis e Permissões para a função do IAM atribuída a AWS Config.

Veja a política: AWS_ ConfigRole.

AWS política gerenciada: AWSConfigUserAccess

Essa política do IAM fornece acesso ao uso AWS Config, incluindo a pesquisa por tags nos recursos e a leitura de todas as tags. Isso não fornece permissão para configuração AWS Config, o que requer privilégios administrativos.

Veja a política: AWSConfigUserAccess.

AWS política gerenciada: ConfigConformsServiceRolePolicy

Para implantar e gerenciar pacotes de conformidade, AWS Config são necessárias permissões do IAM e determinadas permissões de outros serviços. AWS Eles permitem que você implante e gerencie pacotes de conformidade com todas as funcionalidades e são atualizados sempre que AWS Config adicionam novas funcionalidades aos pacotes de conformidade. Consulte Pacotes de conformidade para obter mais informações sobre pacotes de conformidade.

Veja a política: ConfigConformsServiceRolePolítica.

AWS política gerenciada: AWSConfigRulesExecutionRole

Para implantar regras AWS personalizadas do Lambda, AWS Config são necessárias permissões do IAM e determinadas permissões de outros AWS serviços. Eles permitem que AWS Lambda as funções acessem a AWS Config API e os snapshots de configuração que são AWS Config entregues periodicamente ao Amazon S3. Esse acesso é exigido por funções que avaliam as alterações de configuração das regras AWS personalizadas do Lambda e é atualizado sempre que novas funcionalidades são AWS Config adicionadas. Para obter mais informações sobre regras AWS personalizadas do Lambda, consulte Criação de regras e componentes personalizados do AWS Config Lambda de uma regra. AWS Config Para obter mais informações sobre snapshots de configuração, consulte Conceitos | Snapshot de configuração. Para obter mais informações sobre a entrega de snapshots de configuração, consulte Gerenciar o canal de entrega.

Veja a política: AWSConfigRulesExecutionRole.

AWS política gerenciada: AWSConfigMultiAccountSetupPolicy

Para implantar, atualizar e excluir de forma centralizada AWS Config regras e pacotes de conformidade nas contas dos membros de uma organização em AWS Organizations, AWS Config são necessárias permissões do IAM e certas permissões de outros serviços. AWS Essa política gerenciada é atualizada sempre que AWS Config adiciona novas funcionalidades para configuração de várias contas. Para obter mais informações, consulte Gerenciando AWS Config regras em todas as contas em sua organização e Gerenciando pacotes de conformidade em todas as contas em sua organização.

Veja a política: AWSConfigMultiAccountSetupPolicy.

AWS política gerenciada: AWSConfigRoleForOrganizations

Para permitir AWS Config a chamada de AWS Organizations APIs somente para leitura, AWS Config são necessárias permissões do IAM e determinadas permissões de outros serviços. AWS Essa política gerenciada é atualizada sempre que AWS Config adiciona novas funcionalidades para configuração de várias contas. Para obter mais informações, consulte Gerenciando AWS Config regras em todas as contas em sua organização e Gerenciando pacotes de conformidade em todas as contas em sua organização.

Veja a política: AWSConfigRoleForOrganizations.

AWS política gerenciada: AWSConfigRemediationServiceRolePolicy

Para permitir AWS Config a correção de `NON_COMPLIANT` recursos em seu nome, AWS Config são necessárias permissões do IAM e determinadas permissões de outros AWS serviços. Essa política gerenciada é atualizada sempre que AWS Config adiciona novas funcionalidades para remediação. Para obter mais informações sobre remediação, consulte Correção de recursos não compatíveis com regras. AWS Config Para obter mais informações sobre as condições que iniciam os possíveis resultados da AWS Config avaliação, consulte Conceitos | AWS Config Regras.

Veja a política: AWSConfigRemediationServiceRolePolicy.

AWS Config atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS Config desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS Config documento.

Alteração	Descrição	Data
AWS_ConfigRole: adição de elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Essa política agora oferece suporte a permissões adicionais para Amazon Elastic File System (Amazon EFS), Amazon Redshift e. AWS Systems Manager para SAP	17 de junho de 2024
AWSConfigServiceRolePolicy: adição de elasticfilesystem: DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	Essa política agora oferece suporte a permissões adicionais para Amazon Elastic File System (Amazon EFS), Amazon Redshift e. AWS Systems Manager para SAP	17 de junho de 2024
AWS_ConfigRole: adição de "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," " glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetP	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache,, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda, AWS RAM Amazon e Amazon SageMaker Simple Notification Service (Amazon SNS).	22 de fevereiro de 2024

Alteração	Descrição	Data
ermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:GetSMSSandboxAccountStatus"		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache,, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda, AWS RAM Amazon e Amazon SageMaker Simple Notification Service (Amazon SNS).	22 de fevereiro de 2024

Alteração	Descrição	Data
" and "sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess— AWS Config começa a rastrear as alterações dessa política AWS gerenciada	Essa política fornece acesso ao uso AWS Config, incluindo a pesquisa por tags nos recursos e a leitura de todas as tags. Isso não fornece permissão para configuração AWS Config, o que requer privilégios administrativos.	22 de fevereiro de 2024
AWS_ConfigRole: adição de "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Essa política agora oferece suporte a permissões adicionais para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM,AWS Identity and Access Management Amazon Managed Streaming for Apache Kafka (Amazon MSK CloudWatch), Amazon Logs e Amazon Simple Storage Service (AWS Organizations Amazon S3).	5 de dezembro de 2023

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	Essa política agora oferece suporte a permissões adicionais para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM,AWS Identity and Access Management Amazon Managed Streaming for Apache Kafka (Amazon MSK CloudWatch), Amazon Logs e Amazon Simple Storage Service (AWS Organizations Amazon S3).	5 de dezembro de 2023

Alteração	Descrição	Data
AWS_ConfigRole: adição de "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Essa política agora oferece suporte a permissões adicionais para Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB for Redis, Amazon, Amazon AWS Organizations Relational Database Service (QuickSightAmazon RDS), Amazon Redshift, Amazon Route 53, e. AWS Service Catalog AWS Transfer Family	17 de novembro de 2023

Alteração	Descrição	Data
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Alteração	Descrição	Data
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole: adição de "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Essa política agora adiciona identificadores de segurança (SID) para `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` e `AWSConfigSLRApiGatewayStatementID`.	17 de novembro de 2023

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	Essa política agora oferece suporte a permissões adicionais para Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB for Redis, Amazon, Amazon AWS Organizations Relational Database Service (QuickSightAmazon RDS), Amazon Redshift, Amazon Route 53, e. AWS Service Catalog AWS Transfer Family	17 de novembro de 2023

Alteração	Descrição	Data
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

Alteração	Descrição	Data
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy: adição de "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	Essa política agora adiciona identificadores de segurança (SID) para `AWSConfigServiceRolePolicyStatementID`, `AWSConfigSLRLogStatementID`, `AWSConfigSLRLogEventStatementID` e `AWSConfigSLRApiGatewayStatementID`.	17 de novembro de 2023

Alteração	Descrição	Data
AWS_ConfigRole: adição de "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Essa política agora oferece suporte a permissões adicionais para AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently , CloudWatch Amazon Managed Grafana, Amazon, Amazon AWS IoT Inspector GuardDuty,,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS IoT TwinMaker ,,,, e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 de outubro de 2023

Alteração	Descrição	Data
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	Essa política agora oferece suporte a permissões adicionais para AWS Private CA, AWS App Mesh, Amazon Connect, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently , CloudWatch Amazon Managed Grafana, Amazon, Amazon AWS IoT Inspector GuardDuty,,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS IoT TwinMaker ,,,, e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker	4 de outubro de 2023

Alteração	Descrição	Data
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— Remover "ssm:GetParameter"	Essa política agora remove as permissões para AWS Systems Manager (Systems Manager).	6 de setembro de 2023

Alteração	Descrição	Data
AWS_ConfigRole: adição de "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets",	Essa política agora suporta permissões adicionais para AWS App Mesh,, Amazon AWS CloudFormation, Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector ,,,,, Amazon Managed Streaming for Apache Kafka AWS IoT TwinMaker, AWS IoT Wireless Amazon AWS Elemental MediaConnect AWS Network Manager Macie,,,,,,, Amazon Route 53 AWS Organizations Explorador de recursos da AWS, Amazon Simple Storage Service (Amazon S3) e Amazon Simple Notification Serviço (Amazon SNS). AWS IoT	28 de julho de 2023

Alteração	Descrição	Data
"macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "m	Essa política agora oferece suporte a permissões adicionais para Amazon AppStream 2.0 AWS App Mesh,, Amazon AWS CloudFormation,, CloudFront, Amazon Connect AWS CodeArtifact AWS CodeBuild, Amazon, AWS Identity and Access Management (IAM) AWS Glue GuardDuty, Amazon Inspector,,,, Amazon Managed Streaming for Apache Kafka AWS IoT AWS IoT TwinMaker, AWS IoT Wireless Amazon AWS Elemental MediaConnect AWS Network Manager Macie,,,,,,, Amazon Route 53 AWS Organizations Explorador de recursos da AWS, Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) e Amazon EC2 Systems Manager (SSM).	28 de julho de 2023

Alteração	Descrição	Data
acie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

Alteração	Descrição	Data
AWS_ConfigRole: adição de "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	Essa política agora oferece suporte a permissões adicionais para Amazon Connect AWS Amplify AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,,, Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, ,, (IAM), Amazon Managed Streaming for Apache Kafka Streaming for Apache Kafka (AWS Identity and Access Management Amazon MSK AWS IoT Greengrass) AWS Ground Station, Amazon Lightsail, Amazon Logs,, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize, Amazon AWS Migration Hub Refactor Spaces, QuickSight Amazon Simple	13 de junho de 2023

Alteração	Descrição	Data
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "org	Storage Service (Amazon S3), Amazon,. SageMaker AWS Transfer Family	

Alteração	Descrição	Data
anizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	Essa política agora oferece suporte a permissões adicionais para Amazon Connect AWS Amplify AWS App Mesh, Amazon Managed Service for Prometheus, Amazon Athena,,,,, Amazon, Amazon AWS Directory Service DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon CloudWatch Evidently, Amazon Forecast, ,, (IAM), Amazon Managed Streaming for Apache Kafka Streaming for Apache Kafka (AWS Identity and Access Management Amazon MSK AWS IoT Greengrass) AWS Ground Station, Amazon Lightsail, Amazon Logs,, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon AWS Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC), Amazon Personalize, Amazon AWS Migration Hub Refactor Spaces, QuickSight Amazon Simple	13 de junho de 2023

Alteração	Descrição	Data
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAcc	Storage Service (Amazon S3), Amazon,. SageMaker AWS Transfer Family	

Alteração	Descrição	Data
ountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para AWS Amplify, AWS App Mesh, Amazon AWS App Runner CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon,, Amazon AWS Migration Hub Pinpoint AWS Transfer Family, AWS Resilience Hub, Amazon, Directory Service e. SageMaker CloudWatch AWS AWS WAF	13 de abril de 2023

Alteração	Descrição	Data
ion, macie2:GetClassificationExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Alteração	Descrição	Data
AWS_ConfigRole: adição de amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificati	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para AWS Amplify, AWS App Mesh, Amazon AWS App Runner CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon, Amazon AWS Migration Hub Pinpoint AWS Transfer Family, AWS Resilience Hub, Amazon, Directory Service e. SageMaker CloudWatch AWS AWS WAF	13 de abril de 2023

Alteração	Descrição	Data
onExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAML	Essa política agora suporta permissões adicionais para Amazon Managed Workflows para Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon,, CloudFront, CloudWatch, Amazon CloudWatch Evidently AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Forecast,, AWS Identity and Access Management (IAM) AWS Ground Station, Amazon MemoryDB para Redis, AWS IoT Amazon Pinpoint, ,, Amazon AWS Network Manager Relational Database AWS Panorama Service (Amazon RDS), Amazon Redshift e Amazon. SageMaker	30 de março de 2023

Alteração	Descrição	Data
Provider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Alteração	Descrição	Data
AWS_ConfigRole: adição de appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundsta	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon AWS CloudFormation,, CloudFront, CloudWatch AWS CodeArtifact AWS CodeCommit AWS Device Farm, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently, Amazon Forecast,, (IAM AWS IoT) CloudWatch ,, Amazon MemoryDB for Redis, AWS Ground Station Amazon AWS Identity and Access Management Pinpoint,,, AWS Panorama Amazon Relational Database Service Service (Amazon RDS) AWS Network Manager, Amazon Redshift e Amazon. SageMaker	30 de março de 2023

Alteração	Descrição	Data
tion:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

Alteração	Descrição	Data
AWSConfigRulesExecutionRole— AWS Config começa a rastrear as alterações dessa política AWS gerenciada	Essa política permite que AWS Lambda as funções acessem a AWS Config API e os snapshots de configuração que são AWS Config entregues periodicamente ao Amazon S3. Esse acesso é exigido por funções que avaliam as alterações de configuração das regras AWS personalizadas do Lambda.	7 de março de 2023
AWSConfigRoleForOrganizations— AWS Config começa a rastrear as alterações dessa política AWS gerenciada	Essa política permite AWS Config chamar APIs somente para leitura AWS Organizations .	7 de março de 2023
AWSConfigRemediationServiceRolePolicy— AWS Config começa a rastrear as alterações dessa política AWS gerenciada	Essa política permite AWS Config remediar `NON_COMPLIANT` recursos em seu nome.	7 de março de 2023
AWSConfigServiceRolePolicy: adição de auditmanager:GetAccountStatus	Esta política agora concede permissão para retornar o status de registro de uma conta no AWS Audit Manager.	3 de março de 2023
AWS_ConfigRole: adição de auditmanager:GetAccountStatus	Esta política agora concede permissão para retornar o status de registro de uma conta no AWS Audit Manager.	3 de março de 2023

Alteração	Descrição	Data
AWSConfigMultiAccountSetupPolicy— AWS Config começa a rastrear as alterações dessa política AWS gerenciada	Essa política permite AWS Config chamar AWS serviços e implantar AWS Config recursos em uma organização com AWS Organizations.	27 de fevereiro de 2023

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefarm:L	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream , Amazon Kinesis Video Streams AWS HealthLake, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1° de fevereiro de 2023

Alteração	Descrição	Data
istTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Alteração	Descrição	Data
AWS_ConfigRole: adição de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream , Amazon Kinesis Video Streams AWS HealthLake, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1° de fevereiro de 2023

Alteração	Descrição	Data
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: atualização de config:DescribeConfigRules	Como uma prática recomendada de segurança, essa política agora remove uma ampla permissão em nível de recurso para `config:DescribeConfigRules` .	12 de janeiro de 2023

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2) AWS Directory Service,,, Amazon AWS Elemental MediaPackage Lightsail,,, Amazon,, Amazon AWS Glue, AWS IoT, Amazon Route 53 Application Recovery Controller AWS Network Manager, QuickSight Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3) e Amazon Timestream Amazon Timestream.	15 de dezembro de 2022

Alteração	Descrição	Data
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Alteração	Descrição	Data
AWS_ConfigRole: adição de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2) AWS Directory Service,,, Amazon AWS Elemental MediaPackage Lightsail,,, Amazon,, Amazon AWS Glue, AWS IoT, Amazon Route 53 Application Recovery Controller AWS Network Manager, QuickSight Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3) e Amazon Timestream Amazon Timestream.	15 de dezembro de 2022

Alteração	Descrição	Data
Resource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de cloudformation:ListStackResources and cloudformation:ListStacks	Essa política agora concede permissão para retornar descrições de todos os recursos de uma AWS CloudFormation pilha especificada e retornar as informações resumidas das pilhas cujo status corresponda ao especificado. StackStatusFilter	7 de novembro de 2022
AWS_ConfigRole: adição de cloudformation:ListStackResources and cloudformation:ListStacks	Essa política agora concede permissão para retornar descrições de todos os recursos de uma AWS CloudFormation pilha especificada e retornar as informações resumidas das pilhas cujo status corresponda ao especificado. StackStatusFilter	7 de novembro de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersi	Essa política agora oferece suporte a permissões adicionais para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, , AWS AppConfig Amazon Keyspaces AWS Amplify, Amazon, Amazon CloudWatch Connect, Amazon Elastic Compute Cloud (AWS Glue DataBrew Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon, EventBridge Amazon Location Service, AWS Fault Injection Service Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,,, Amazon AWS IoT, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security Token Service	19 de outubro de 2022

Alteração	Descrição	Data
ons, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsite		

Alteração	Descrição	Data
wise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage		

Alteração	Descrição	Data
, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Alteração	Descrição	Data
AWS_ConfigRole: adição de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVersions, databrew:ListRulesets,	Essa política agora oferece suporte a permissões adicionais para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, , AWS AppConfig Amazon Keyspaces AWS Amplify, Amazon, Amazon CloudWatch Connect, Amazon Elastic Compute Cloud (AWS Glue DataBrew Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon, EventBridge Amazon Location Service, AWS Fault Injection Service Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,,, Amazon AWS IoT, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security Token Service	19 de outubro de 2022

Alteração	Descrição	Data
databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsit		

Alteração	Descrição	Data
ewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails, panorama:DescribePackage, panorama:Describe		

Alteração	Descrição	Data
PackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de Glue::GetTable	Essa política agora concede permissão para recuperar a definição de AWS Glue tabela em um catálogo de dados para uma tabela especificada.	14 de setembro de 2022
AWS_ConfigRole: adição de Glue::GetTable	Essa política agora concede permissão para recuperar a definição de AWS Glue tabela em um catálogo de dados para uma tabela especificada.	14 de setembro de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirr	Essa política agora oferece suporte a permissões adicionais para Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Schemas, Amazon Fraud Detector, Amazon EventBridge, EventBridge Amazon GameLift Interactive Video Service (Amazon IVS) Amazon FinSpace, Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon Route 53 Resolver Controlador de Recuperação de Aplicativos QuickSigh	7 de setembro de 2022

Alteração	Descrição	Data
orFilters, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, game	t Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,, ,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, AWS Transfer Family e.	

Alteração	Descrição	Data
lift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:Desc		

Alteração	Descrição	Data
ribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, ioteventsnts:DescribeAlarmModel, ioteventsents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, ioteventsents:ListDetectorModels, iotevents:ListInputs, ioteventsents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets		

Alteração	Descrição	Data
, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:Ge		

Alteração	Descrição	Data
tInstance, lightsail:GetInst ances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, l ightsail:GetLoadBalancers, l ightsail:GetLoadBalancerTls Certificates, lightsail:GetS taticIp, lightsail:GetStaticIps, lookoutequipment:Descri beInferenceScheduler, lookoutequipment:ListTag sForResource, lookoutmetrics :DescribeAlert, lookoutmetri cs:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, l ookoutmetrics:ListAnomalyDe tectors, lookoutmetrics:List MetricSets, lookoutmetrics:L istTagsForResource, lookoutv ision:DescribeProject, looko utvision:ListProjects, manag edblockchain:GetMember, managedblockchain:GetN etwork, managedbloc kchain:GetNode, man agedblockchain:ListInvitati ons, managedblockch ain:ListMembers, ma nagedblockchain:ListNodes, mediapackage-vod:De scribePackagingGroup, mediapackage-vod:ListPac kagingGroups, media package-vod:ListTagsForReso urce, mobiletargeting:GetInA ppTemplate, mobiletargeting:		

Alteração	Descrição	Data
ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies,		

Alteração	Descrição	Data
route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPo		

Alteração	Descrição	Data
intPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUs		

Alteração	Descrição	Data
er, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Alteração	Descrição	Data
AWS_ConfigRole: adição de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets,	Essa política agora oferece suporte a permissões adicionais para Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Schemas, Amazon Fraud Detector, Amazon EventBridge, EventBridge Amazon GameLift Interactive Video Service (Amazon IVS) Amazon FinSpace, Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon Route 53 Resolver Controlador de Recuperação de Aplicativos QuickSigh	7 de setembro de 2022

Alteração	Descrição	Data
ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamel	t Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream,,,,,,,, ,,,,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, e AWS Transfer Family	

Alteração	Descrição	Data
ift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination		

Alteração	Descrição	Data
, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwi		

Alteração	Descrição	Data
nmaker:ListEntities, iottwin maker:ListScenes, iottwinmak er:ListTagsForResource, iott winmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfigura tion, ivs:GetStreamKey, ivs:ListChannels, ivs:Li stPlaybackKeyPairs, ivs:List RecordingConfigurations, ivs:ListStreamKeys, iv s:ListTagsForResource, kines isanalytics:ListApplications, lakeformation:DescribeRes ource, lakeformation:GetData LakeSettings, lakeformation: ListPermissions, lakeformati on:ListResources, lex:Descri beBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:List BotLocales, lex:ListBots, lex :ListTagsForResource, licens e-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLice nses, license-manager:ListRe ceivedGrants, lightsail:GetA larms, lightsail:GetBuckets, lightsail:GetCertificates, l ightsail:GetDisk, lightsail: GetDisks, lightsail:GetInsta nce, lightsail:GetInstances, lightsail:GetKeyPair, lights		

Alteração	Descrição	Data
ail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile,		

Alteração	Descrição	Data
nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetRead		

Alteração	Descrição	Data
inessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPointPolicy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetL		

Alteração	Descrição	Data
ifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:		

Alteração	Descrição	Data
ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream , Amazon Kinesis Video Streams AWS HealthLake, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1° de fevereiro de 2023

Alteração	Descrição	Data
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

Alteração	Descrição	Data
AWS_ConfigRole: adição de airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	Essa política agora oferece suporte a permissões adicionais para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream , Amazon Kinesis Video Streams AWS HealthLake, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch	1° de fevereiro de 2023

Alteração	Descrição	Data
m:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy: atualização de config:DescribeConfigRules	Como uma prática recomendada de segurança, essa política agora remove uma ampla permissão em nível de recurso para `config:DescribeConfigRules` .	12 de janeiro de 2023

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2) AWS Directory Service,,, Amazon AWS Elemental MediaPackage Lightsail,,, Amazon,, Amazon AWS Glue, AWS IoT, Amazon Route 53 Application Recovery Controller AWS Network Manager, QuickSight Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3) e Amazon Timestream Amazon Timestream.	15 de dezembro de 2022

Alteração	Descrição	Data
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Alteração	Descrição	Data
AWS_ConfigRole: adição de APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	Essa política agora oferece suporte a permissões adicionais para o Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2) AWS Directory Service,,, Amazon AWS Elemental MediaPackage Lightsail,,, Amazon,, Amazon AWS Glue, AWS IoT, Amazon Route 53 Application Recovery Controller AWS Network Manager, QuickSight Amazon Simple Storage Service (AWS Resource Access Manager Amazon S3) e Amazon Timestream Amazon Timestream.	15 de dezembro de 2022

Alteração	Descrição	Data
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de cloudformation:ListStackResources and cloudformation:ListStacks	Essa política agora concede permissão para retornar descrições de todos os recursos de uma AWS CloudFormation pilha especificada e retornar as informações resumidas das pilhas cujo status corresponda ao especificado. StackStatusFilter	7 de novembro de 2022
AWS_ConfigRole: adição de cloudformation:ListStackResources and cloudformation:ListStacks	Essa política agora concede permissão para retornar descrições de todos os recursos de uma AWS CloudFormation pilha especificada e retornar as informações resumidas das pilhas cujo status corresponda ao especificado. StackStatusFilter	7 de novembro de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Essa política agora oferece suporte a permissões adicionais para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, , AWS AppConfig Amazon Keyspaces AWS Amplify, Amazon, Amazon CloudWatch Connect, Amazon Elastic Compute Cloud (AWS Glue DataBrew Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon, EventBridge Amazon Location Service, AWS Fault Injection Service Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,,, Amazon AWS IoT, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security Token Service	19 de outubro de 2022

Alteração	Descrição	Data
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Alteração	Descrição	Data
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Alteração	Descrição	Data
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Alteração	Descrição	Data
AWS_ConfigRole: adição de acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	Essa política agora oferece suporte a permissões adicionais para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, , AWS AppConfig Amazon Keyspaces AWS Amplify, Amazon, Amazon CloudWatch Connect, Amazon Elastic Compute Cloud (AWS Glue DataBrew Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon, Amazon Fraud Detector, Amazon FSx, Amazon, EventBridge Amazon Location Service, AWS Fault Injection Service Amazon Lex, Amazon Lightsail, GameLift Amazon Pinpoint,,,, Amazon AWS IoT, Amazon Relational Database Service (Amazon RDS), AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Amazon AWS RoboMaker Rekognition AWS Resource Groups,,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security Token Service	19 de outubro de 2022

Alteração	Descrição	Data
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

Alteração	Descrição	Data
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

Alteração	Descrição	Data
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de Glue::GetTable	Essa política agora concede permissão para recuperar a definição de AWS Glue tabela em um catálogo de dados para uma tabela especificada.	14 de setembro de 2022
AWS_ConfigRole: adição de Glue::GetTable	Essa política agora concede permissão para recuperar a definição de AWS Glue tabela em um catálogo de dados para uma tabela especificada.	14 de setembro de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorFilte	Essa política agora oferece suporte a permissões adicionais para Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Schemas, Amazon Fraud Detector, Amazon EventBridge, EventBridge Amazon GameLift Interactive Video Service (Amazon IVS) Amazon FinSpace, Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon Route 53 Resolver Controlador de Recuperação de Aplicativos QuickSigh	7 de setembro de 2022

Alteração	Descrição	Data
rs, ec2:DescribeTrafficMirrorTargets, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity,	t Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream AWS AppConfig,,,,,,,,,,,,,,,,,,,,,,, AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation AWS License Manager, AWS Resilience Hub, AWS Signer, AWS Transfer Family e.	

Alteração	Descrição	Data
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

Alteração	Descrição	Data
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

Alteração	Descrição	Data
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

Alteração	Descrição	Data
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

Alteração	Descrição	Data
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

Alteração	Descrição	Data
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

Alteração	Descrição	Data
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

Alteração	Descrição	Data
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

Alteração	Descrição	Data
AWS_ConfigRole: adição de appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	Essa política agora oferece suporte a permissões adicionais para Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Schemas, Amazon Fraud Detector, Amazon EventBridge, EventBridge Amazon GameLift Interactive Video Service (Amazon IVS) Amazon FinSpace, Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble StudioAmazon Pinpoint, Amazon, Amazon Route 53 Resolver Controlador de Recuperação de Aplicativos QuickSigh	7 de setembro de 2022

Alteração	Descrição	Data
ts, ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	t Amazon Route 53, Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestream AWS AppConfig,,,,,,,,,,,,,,,,,,,,,,, AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker AWS Lake Formation, AWS License Manager, AWS Resilience Hub, AWS Signer, e AWS Transfer Family	

Alteração	Descrição	Data
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

Alteração	Descrição	Data
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

Alteração	Descrição	Data
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

Alteração	Descrição	Data
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

Alteração	Descrição	Data
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

Alteração	Descrição	Data
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

Alteração	Descrição	Data
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

Alteração	Descrição	Data
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy: adição de datasync:ListAgent s, datasync:ListLocations, datasync:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	Essa política agora concede permissão para retornar uma lista de AWS DataSync agentes, locais de DataSync origem e destino e DataSync tarefas em um Conta da AWS; listar informações resumidas sobre os AWS Cloud Map namespaces e serviços associados a um ou mais namespaces especificados em um Conta da AWS; e listar todas as listas de contatos do Amazon Simple Email Service (Amazon SES) disponíveis em. Conta da AWS	22 de agosto de 2022

Alteração	Descrição	Data
AWS_ConfigRole: adição de datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	Essa política agora concede permissão para retornar uma lista de AWS DataSync agentes, locais de DataSync origem e destino e DataSync tarefas em um Conta da AWS; listar informações resumidas sobre os AWS Cloud Map namespaces e serviços associados a um ou mais namespaces especificados em um Conta da AWS; e listar todas as listas de contatos do Amazon Simple Email Service (Amazon SES) disponíveis em. Conta da AWS	22 de agosto de 2022
ConfigConformsServiceRolePolicy: adição de cloudwatch:PutMetricData	Essa política agora concede permissão para publicar pontos de dados métricos na Amazon CloudWatch.	25 de julho de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	Essa política agora oferece suporte a permissões adicionais para Amazon Elastic Container Service (Amazon ECS), Amazon, ElastiCache Amazon, EventBridge Amazon FSx, Amazon Managed Service para Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon, Amazon Rekognition, QuickSight Amazon Simple Serviço de armazenamento (AWS RoboMaker Amazon S3), Amazon Simple Email Service AWS Amplify(Amazon SES),,,,,,, (IAM Identity Center), EC2 Image Builder e Elastic Load AWS DataSync AWS Firewall Manager Balancing. AWS AppConfig AWS AppSync AWS Billing Conductor AWS Glue AWS IAM Identity Center	15 de julho de 2022

Alteração	Descrição	Data
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

Alteração	Descrição	Data
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Alteração	Descrição	Data
sso:GetInlinePolicyForPermissionSet		

Alteração	Descrição	Data
AWS_ConfigRole: adição de amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	Essa política agora oferece suporte a permissões adicionais para Amazon Elastic Container Service (Amazon ECS), Amazon, ElastiCache Amazon, EventBridge Amazon FSx, Amazon Managed Service para Apache Flink, Amazon Location Service, Amazon Managed Streaming for Apache Kafka, Amazon, Amazon Rekognition, QuickSight Amazon Simple Serviço de armazenamento (AWS RoboMaker Amazon S3), Amazon Simple Email Service AWS Amplify(Amazon SES),,,,,,, (IAM Identity Center), EC2 Image Builder e Elastic Load AWS DataSync AWS Firewall Manager Balancing. AWS AppConfig AWS AppSync AWS Billing Conductor AWS Glue AWS IAM Identity Center	15 de julho de 2022

Alteração	Descrição	Data
scribeLocationS3, datasync: DescribeLocationSmb, datasy nc:DescribeTask, datasync: ListTagsForResource, ecr:De scribePullThroughCacheRules , ecr:DescribeRegistry, ecr:G etRegistryPolicy, elasticac he:DescribeCacheParameters, elasticloadbalancing:Descr ibeListenerCertificates, el asticloadbalancing:Describe TargetGroupAttributes, elas ticloadbalancing:DescribeTa rgetGroups, elasticloadbala ncing:DescribeTargetHealth, events:DescribeApiDestinat ion, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListP olicies, fms:ListTagsForRes ource, fsx:DescribeVolumes, geo:DescribeGeofenceColl ection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator , geo:DescribeTracker, geo:ListTrackerConsumers, g lue:BatchGetJobs, glue:Batc hGetWorkflows, glue:GetC rawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuil der: GetComponent, imagebuil der: ListComponentBuildVers ions, imagebuilder: ListCompo		

Alteração	Descrição	Data
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

Alteração	Descrição	Data
sso:GetInlinePolicyForPermissionSet		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAtt	Essa política agora concede permissão para obter um catálogo de dados específico do Amazon Athena, listar os catálogos de dados do Athena em um e listar as tags associadas a um Conta da AWS grupo de trabalho ou recurso do catálogo de dados do Athena; para obter uma lista dos gráficos de comportamento do Amazon Detective e as tags de um gráfico de comportamento do Detective; obter uma lista de metadados de recursos para uma determinada lista de nomes de endpoints de desenvolvimento, obter informações sobre um determinado endpoint AWS Glue de desenvolvimento, obtenha todos os endpoints de desenvolvimento em um, recupere uma segurança AWS Glue especificada AWS Glue Conta da AWS AWS Glue configuração, obtenha todas as configurações de AWS Glue segurança, obtenha uma lista de tags associadas a um AWS Glue recurso, obtenha informações sobre um AWS Glue grupo de	31 de maio de 2022

Alteração	Descrição	Data
ributeConfiguration, sso:DescribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	trabalho com o nome especificado, recupere os nomes de todos os recursos do AWS Glue rastreador em uma AWS conta, obtenha os nomes de todos os recursos em uma, liste os nomes de todos os AWS Glue `DevEndpoint` recursos de AWS Glue trabalho em uma Conta da AWS, obtenha detalhes sobre contas de AWS Glue membros Conta da AWS, liste nomes de AWS Glue fluxos de trabalho criados em uma conta e liste grupos de trabalho disponíveis para uma conta; AWS Glue para recuperar detalhes sobre um GuardDuty filtro da Amazon, recuperar um GuardDuty IPSet, recuperar um GuardDuty ThreatIntelSet, recuperar contas de GuardDuty membros, obter uma lista de GuardDuty filtros, obter os IPSets do GuardDuty serviço, recuperar tags para o Serviço e obter as do GuardDuty serviço; para obter o status atual e as definições ThreatIntelSets de configuração de uma conta Amazon Macie; para recuperar o recurso e as associações	

Alteração	Descrição	Data
	principais para AWS Resource Access Manager (AWS RAM) compartilhamentos de recursos e recuperar detalhes sobre compartilhamentos de recursos; para GuardDuty AWS RAM obtenha informaçõ es sobre um conjunto de configurações existente do Amazon Simple Email Service (Amazon SES), obtenha uma lista de destinos de eventos associados a um conjunto de configurações do Amazon SES e liste todos os conjuntos de configuração associado s a uma conta do Amazon SES; e para obter uma lista dos atributos do diretório do Identity Center, obtenha os detalhes de AWS IAM Identity Center um conjunto de permissões, obtenha a política gerenciada do IAM que está anexada a um conjunto de permissões especificado do IAM Identity Center, obtenha as permissões definidas para uma instância do IAM Identity Center e obter tags para o IAM Identity Center recursos.	

Alteração	Descrição	Data
AWS_ConfigRole: adição de athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	Essa política agora concede permissão para obter um catálogo de dados específico do Amazon Athena, listar os catálogos de dados do Athena em um e listar as tags associadas a um Conta da AWS grupo de trabalho ou recurso do catálogo de dados do Athena; para obter uma lista dos gráficos de comportamento do Amazon Detective e as tags de um gráfico de comportamento do Detective; obter uma lista de metadados de recursos para uma determinada lista de nomes de endpoints de desenvolvimento, obter informações sobre um determinado endpoint AWS Glue de desenvolvimento, obtenha todos os endpoints de desenvolvimento em um, recupere uma segurança AWS Glue especificada AWS Glue Conta da AWS AWS Glue configuração, obtenha todas as configurações de AWS Glue segurança, obtenha uma lista de tags associadas a um AWS Glue recurso, obtenha informações sobre um AWS Glue grupo de	31 de maio de 2022

Alteração	Descrição	Data
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	trabalho com o nome especificado, recupere os nomes de todos os recursos do AWS Glue rastreador em uma AWS conta, obtenha os nomes de todos os recursos em uma, liste os nomes de todos os AWS Glue `DevEndpoint` recursos de AWS Glue trabalho em uma Conta da AWS, obtenha detalhes sobre contas de AWS Glue membros Conta da AWS, liste nomes de AWS Glue fluxos de trabalho criados em uma conta e liste grupos de trabalho disponíveis para uma conta; AWS Glue para recuperar detalhes sobre um GuardDuty filtro da Amazon, recuperar um GuardDuty IPSet, recuperar um GuardDuty ThreatIntel Set, recuperar contas de GuardDuty membros, obter uma lista de GuardDuty filtros, obter os IPSets do GuardDuty serviço, recuperar tags para o Serviço e obter as do GuardDuty serviço; para obter o status atual e as definições ThreatIntelSets de configuração de uma conta Amazon Macie; para recuperar o recurso e as associações	

Alteração	Descrição	Data
	principais para AWS Resource Access Manager (AWS RAM) compartilhamentos de recursos e recuperar detalhes sobre compartilhamentos de recursos; para GuardDuty AWS RAM obtenha informaçõ es sobre um conjunto de configurações existente do Amazon Simple Email Service (Amazon SES), obtenha uma lista de destinos de eventos associados a um conjunto de configurações do Amazon SES e liste todos os conjuntos de configuração associado s a uma conta do Amazon SES; e para obter uma lista dos atributos do diretório do Identity Center, obtenha os detalhes de AWS IAM Identity Center um conjunto de permissões, obtenha a política gerenciada do IAM que está anexada a um conjunto de permissões especificado do IAM Identity Center, obtenha as permissões definidas para uma instância do IAM Identity Center e obter tags para o IAM Identity Center recursos.	

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Essa política agora concede permissão para obter informações sobre todo ou um armazenamento de dados de AWS CloudTrail eventos (EDS) específico, obter informações sobre todo ou um AWS CloudFormation recurso específico, obter uma lista de um grupo de parâmetros ou grupo de sub-rede do DynamoDB Accelerator (DAX), obter informações AWS Database Migration Service sobre AWS DMS() tarefas de replicação para sua conta na região atual que está sendo acessada e obter uma lista de todas as políticas de um tipo específico. AWS Organizations	7 de abril de 2022

Alteração	Descrição	Data
AWS_ConfigRole: adição de cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	Essa política agora concede permissão para obter informações sobre todo ou um armazenamento de dados de AWS CloudTrail eventos (EDS) específico, obter informações sobre todo ou um AWS CloudFormation recurso específico, obter uma lista de um grupo de parâmetros ou grupo de sub-rede do DynamoDB Accelerator (DAX), obter informações AWS Database Migration Service sobre AWS DMS() tarefas de replicação para sua conta na região atual que está sendo acessada e obter uma lista de todas as políticas de um tipo específico. AWS Organizations	7 de abril de 2022

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	Essa política agora oferece suporte a permissões adicionais para AWS Backup, AWS Batch, DynamoDB Accelerator, Amazon DynamoDB, AWS Database Migration Service Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx GuardDuty, Amazon,,, Amazon Relational Database Service, V2 e Amazon. AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 de março de 2022

Alteração	Descrição	Data
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Alteração	Descrição	Data
AWS_ConfigRole: adição de backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	Essa política agora oferece suporte a permissões adicionais para AWS Backup, AWS Batch, DynamoDB Accelerator, Amazon DynamoDB, AWS Database Migration Service Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Kubernetes Service, Amazon FSx GuardDuty, Amazon,,, Amazon Relational Database Service, V2 e Amazon. AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	14 de março de 2022

Alteração	Descrição	Data
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição de elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Essa política agora concede permissão para obter detalhes sobre os ambientes do Elastic Beanstalk e uma descrição das configurações do conjunto de configurações especificado do Elastic Beanstalk, obter um mapa das versões do Elasticsearch, descrever os grupos de opções disponíveis OpenSearch do Amazon RDS para um banco de dados e obter informações sobre uma configuração de implantação. CodeDeploy Agora, essa política também concede permissão para recuperar o contato alternativo especificado anexado a uma Conta da AWS, recuperar informações sobre uma AWS Organizations política, recuperar uma política de repositório do Amazon ECR, recuperar informações sobre uma regra arquivada AWS Config , recuperar uma lista de famílias de definição de tarefas do Amazon ECS, listar as unidades organizacionais (OUs) raiz ou principal da OU ou conta secundária especificada e listar as políticas anexadas à raiz,	10 de fevereiro de 2022

Alteração	Descrição	Data
	unidade organizacional ou conta de destino especificada.	

Alteração	Descrição	Data
AWS_ConfigRole: adição de elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	Essa política agora concede permissão para obter detalhes sobre os ambientes do Elastic Beanstalk e uma descrição das configurações do conjunto de configurações especificado do Elastic Beanstalk, obter um mapa das versões do Elasticsearch, descrever os grupos de opções disponíveis OpenSearch do Amazon RDS para um banco de dados e obter informações sobre uma configuração de implantação. CodeDeploy Agora, essa política também concede permissão para recuperar o contato alternativo especificado anexado a uma Conta da AWS, recuperar informações sobre uma AWS Organizations política, recuperar uma política de repositório do Amazon ECR, recuperar informações sobre uma regra arquivada AWS Config , recuperar uma lista de famílias de definição de tarefas do Amazon ECS, listar as unidades organizacionais (OUs) raiz ou principal da OU ou conta secundária especificada e listar as políticas anexadas à raiz,	10 de fevereiro de 2022

Alteração	Descrição	Data
	unidade organizacional ou conta de destino especificada.	
AWSConfigServiceRolePolicy: adição de logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Essa política agora concede permissão para criar grupos e fluxos de CloudWatch log da Amazon e para gravar registros em fluxos de log criados.	15 de dezembro de 2021
AWS_ConfigRole: adição de logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	Essa política agora concede permissão para criar grupos e fluxos de CloudWatch log da Amazon e para gravar registros em fluxos de log criados.	15 de dezembro de 2021
AWSConfigServiceRolePolicy: adição de es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Essa política agora concede permissão para obter detalhes sobre um domínio/domínios do Amazon OpenSearch Service (OpenSearch Service) e obter uma lista detalhada de parâmetros para um determinado grupo de parâmetros de banco de dados do Amazon Relational Database Service (Amazon RDS). Essa política também concede permissão para obter detalhes sobre os ElastiCache snapshots da Amazon.	8 de setembro de 2021

Alteração	Descrição	Data
AWS_ConfigRole: adição de es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	Essa política agora concede permissão para obter detalhes sobre um domínio/domínios do Amazon OpenSearch Service (OpenSearch Service) e obter uma lista detalhada de parâmetros para um determinado grupo de parâmetros de banco de dados do Amazon Relational Database Service (Amazon RDS). Essa política também concede permissão para obter detalhes sobre os ElastiCache snapshots da Amazon.	8 de setembro de 2021

Alteração	Descrição	Data
AWSConfigServiceRolePolicy— Adicionar logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine e permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para listar as tags de um grupo de logs, listar as tags de uma máquina de estado e listar todas as máquinas de estado. Essa política agora concede permissão para obter detalhes sobre uma máquina de estado. Agora, essa política também oferece suporte a permissões adicionais para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	28 de julho de 2021

Alteração	Descrição	Data
AWS_ConfigRole— Adicione l ogs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine e permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para listar as tags de um grupo de logs, listar as tags de uma máquina de estado e listar todas as máquinas de estado. Essa política agora concede permissão para obter detalhes sobre uma máquina de estado. Agora, essa política também oferece suporte a permissões adicionais para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service A WS Global Accelerator AWS Storage Gateway	28 de julho de 2021

Alteração	Descrição	Data
AWSConfigServiceRolePolicy— Adicionar ssm:DescribeDocumentPermission permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para visualizar as permissões de documentos e informações do AWS Systems Manager sobre o IAM Access Analyzer. Essa política agora oferece suporte a tipos de AWS recursos adicionais para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessárias para oferecer suporte a esses tipos de recursos. Agora, essa política também oferece suporte à filtragem de funções do Lambda @Edge para a regra gerenciada AWS Config lambda-inside-vpc.	8 de junho de 2021

Alteração	Descrição	Data
AWS_ConfigRole— Adicionar ssm:DescribeDocumentPermission permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para visualizar as permissões de documentos e informações do AWS Systems Manager sobre o IAM Access Analyzer. Essa política agora oferece suporte a tipos de AWS recursos adicionais para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessárias para oferecer suporte a esses tipos de recursos. Agora, essa política também oferece suporte à filtragem de funções do Lambda @Edge para a regra gerenciada AWS Config lambda-inside-vpc.	8 de junho de 2021

Alteração	Descrição	Data
AWSConfigServiceRolePolicy: adição da permissão apigateway:GET para fazer chamadas GET somente leitura para o API Gateway e adição das permissões s3:GetAccessPointPolicy e s3:GetAccessPointPolicyStatus para invocar as APIs somente leitura do Amazon S3.	Essa política agora concede permissões que permitem fazer chamadas GET somente AWS Config para leitura para o API Gateway para dar suporte a uma AWS Config regra para o API Gateway. A política também adiciona permissões que permitem AWS Config invocar as APIs somente para leitura do Amazon Simple Storage Service (Amazon S3), que são necessárias para oferecer suporte ao novo tipo de recurso. `AWS::S3::AccessPoint`	10 de maio de 2021
AWS_ ConfigRole — Adicione apigateway:GET permissão para fazer chamadas GET somente para leitura para o API Gateway e s3:GetAccessPointPolicy permissão e s3:GetAccessPointPolicyStatus permissão para invocar APIs somente para leitura do Amazon S3	Essa política agora concede permissões que permitem fazer chamadas GET somente AWS Config para leitura para o API Gateway para dar suporte a um AWS Config para o API Gateway. A política também adiciona permissões que permitem AWS Config invocar as APIs somente para leitura do Amazon Simple Storage Service (Amazon S3), que são necessárias para oferecer suporte ao novo tipo de recurso. `AWS::S3::AccessPoint`	10 de maio de 2021

Alteração	Descrição	Data
AWSConfigServiceRolePolicy— Adicionar ssm:ListDocuments permissão e permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para exibir informações sobre documentos especificados do AWS Systems Manager . Agora AWS Backup, essa política também oferece suporte a tipos de AWS recursos adicionais para Amazon Elastic File System ElastiCache, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessárias para oferecer suporte a esses tipos de recursos.	1º de abril de 2021

Alteração	Descrição	Data
AWS_ConfigRole— Adicionar ssm:ListDocuments permissão e permissões adicionais para tipos AWS de recursos	Esta política agora concede permissão para exibir informações sobre documento s especificados do AWS Systems Manager . Agora AWS Backup, essa política também oferece suporte a tipos de AWS recursos adicionais para Amazon Elastic File System ElastiCac he, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessári as para oferecer suporte a esses tipos de recursos.	1º de abril de 2021
`AWSConfigRole` está obsoleto	`AWSConfigRole` está obsoleto. A política de substituição é `AWS_Confi gRole` .	1º de abril de 2021
AWS Config começou a rastrear as alterações	AWS Config começou a rastrear as mudanças em suas políticas AWS gerenciad as.	1º de abril de 2021

Permissões para a função do IAM atribuída a AWS Config

Uma função do IAM permite que você defina um conjunto de permissões. AWS Config assume a função que você atribui a ele para gravar em seu bucket do S3, publicar em seu tópico do SNS e fazer `Describe` solicitações de `List` API para obter detalhes de configuração de seus recursos. AWS Para obter mais informações sobre funções do IAM, consulte Perfis do IAM no Guia do usuário do IAM.

Quando você usa o AWS Config console para criar ou atualizar uma função do IAM, anexa AWS Config automaticamente as permissões necessárias para você. Para ter mais informações, consulte Configurando AWS Config com o console.

Sumário

- Criar políticas do perfil do IAM
  - Adicionar uma política de confiança do IAM à sua função
  - Política de perfil do IAM para o bucket do S3
  - Política de perfil do IAM para chave do KMS
  - Política de perfil do IAM para o tópico do Amazon SNS
  - Política de perfil do IAM para obter detalhes de configuração
- Gerenciar permissões para gravação de bucket do S3

Criar políticas do perfil do IAM

Quando você usa o AWS Config console para criar uma função do IAM, anexa AWS Config automaticamente as permissões necessárias à função para você.

Se você estiver usando o AWS CLI para configurar AWS Config ou estiver atualizando uma função existente do IAM, você deve atualizar manualmente a política para permitir o acesso AWS Config ao bucket do S3, publicar no tópico do SNS e obter detalhes de configuração sobre seus recursos.

Adicionar uma política de confiança do IAM à sua função

Você pode criar uma política de confiança do IAM que AWS Config permita assumir uma função e usá-la para monitorar seus recursos. Para obter mais informações sobre políticas de confiança, consulte Termos e conceitos dos perfis no Guia do usuário do IAM.

Veja a seguir um exemplo de política de confiança para AWS Config funções:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Você pode usar a condição `AWS:SourceAccount` na relação de confiança acima do perfil do IAM para restringir a entidade principal de serviço do Config a interagir somente com o perfil do IAM da AWS ao realizar operações em nome de contas específicas.

AWS Config também suporta a `AWS:SourceArn` condição que restringe o responsável pelo serviço Config a assumir apenas a função do IAM ao realizar operações em nome da conta proprietária. Ao usar o principal de AWS Config serviço, a `AWS:SourceArn` propriedade sempre será definida como `arn:aws:config:sourceRegion:sourceAccountID:*` onde `sourceRegion` está a região do gravador de configuração e `sourceAccountID` é a ID da conta que contém o gravador de configuração. Para obter mais informações sobre o gravador AWS Config de configuração, consulte Gerenciando o gravador de configuração. Por exemplo, adicione a seguinte condição para restringir a entidade principal do serviço Config a assumir apenas o perfil do IAM somente em nome de um gravador de configuração na região `us-east-1` na conta`123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Política de perfil do IAM para o bucket do S3

O exemplo de política a seguir concede AWS Config permissão para acessar seu bucket do S3:

```
{
  "Version":"2012-10-17",
  "Statement":[
```

```
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

Política de perfil do IAM para chave do KMS

O exemplo de política a seguir concede AWS Config permissão para usar criptografia baseada em KMS em novos objetos para entrega de buckets do S3:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

Política de perfil do IAM para o tópico do Amazon SNS

O exemplo de política a seguir concede AWS Config permissão para acessar seu tópico do SNS:

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

Se o tópico do SNS for criptografado, para obter mais instruções de configuração, consulte Configuração de permissões do AWS KMS no Guia do desenvolvedor do Amazon Simple Notification Service.

Política de perfil do IAM para obter detalhes de configuração

Para registrar suas configurações AWS de recursos, AWS Config são necessárias permissões do IAM para obter os detalhes de configuração sobre seus recursos.

Use a política AWS gerenciada AWS_ ConfigRole e anexe-a à função do IAM à qual você atribui. AWS Config AWS atualiza essa política sempre que AWS Config adiciona suporte para um tipo de AWS recurso, o que significa que AWS Config continuará a ter as permissões necessárias para obter detalhes de configuração, desde que a função tenha essa política gerenciada anexada.

Se você criar ou atualizar uma função com o console, AWS Config anexará o AWS_ ConfigRole para você.

Se você usar o AWS CLI, use o **`attach-role-policy`** comando e especifique o Amazon Resource Name (ARN) para AWS_: ConfigRole

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
```

Gerenciar permissões para gravação de bucket do S3

AWS Config registra e entrega notificações quando um bucket do S3 é criado, atualizado ou excluído.

É recomendável que você use `AWSServiceRoleForConfig` (consulte Using Service-Linked Roles for AWS Config) ou um perfil do IAM personalizado utilizando a política gerenciada `AWS_ConfigRole`. Para obter mais informações sobre as práticas recomendadas para a gravação de configuração, consulte Práticas recomendadas do AWS Config.

Se você precisar gerenciar permissões em nível de objeto para a gravação do bucket, certifique-se de fornecer `config.amazonaws.com` (o nome principal do AWS Config serviço) acesso a todas as permissões relacionadas ao S3 da política gerenciada. `AWS_ConfigRole` Para obter mais informações, consulte Permissões para buckets do Amazon S3.

Atualização da função do IAM atribuída a AWS Config

Você pode atualizar a função do IAM assumida a AWS Config qualquer momento. Antes de atualizar o perfil do IAM crie um novo perfil para substituir o antigo. Você deve anexar políticas à nova função que concedam permissões AWS Config para registrar configurações e entregá-las ao seu canal de entrega. Além disso, copie o nome do recurso da Amazon (ARN) de seu novo perfil do IAM. Você precisará dele para atualizar o perfil do IAM. Para obter informações sobre a criação de um perfil do IAM e anexar políticas necessárias para o perfil do IAM consulte Criar um perfil do IAM.

> **Note**
>
> Para encontrar o ARN de um perfil do IAM existente, acesse o console do IAM em https://console.aws.amazon.com/iam/. Selecione Roles (Funções) no painel de navegação. Em seguida, escolha o nome da função desejada e localize o ARN na parte superior da página Summary (Resumo).

Atualizar o perfil do IAM

Você pode atualizar sua função do IAM usando o AWS Management Console ou AWS CLI o.

To update the IAM role (Console)

Se você estiver usando AWS Config em uma região que ofereça suporte a AWS Config regras, conclua as etapas a seguir. Para obter a lista das regiões compatíveis, consulte Regiões e endpoints do AWS Config no Referência geral da Amazon Web Services.

1. Faça login no AWS Management Console e abra o AWS Config console em https://console.aws.amazon.com/config/.
2. Selecione Configurações no painel de navegação.
3. Escolha Editar na página Configurações.
4. Na seção Governança de dados, escolha a função do IAM para AWS Config:
   - Use uma função AWS Config vinculada ao serviço existente — AWS Config cria uma função com as permissões necessárias.
   - Escolha uma função da sua conta — Para funções existentes, escolha uma função do IAM em sua conta.
5. Escolha Salvar.

To update the IAM role (AWS CLI)

Use o comando `put-configuration-recorder` e especifique o Nome de recurso da Amazon (ARN) da nova função:

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

Permissões para o bucket Amazon S3 para o AWS Config canal de entrega

> **Important**
>
> Esta página trata da configuração do Amazon S3 Bucket para o canal de AWS Config entrega. Esta página não trata do tipo de `AWS::S3::Bucket` recurso que o gravador AWS Config de configuração pode registrar. Para obter mais informações sobre o canal AWS Config de entrega, consulte Gerenciando o canal de entrega.

Por padrão, todos os buckets e objetos do Amazon S3 são privados. Somente o proprietário do recurso Conta da AWS que criou o bucket pode acessar esse bucket. No entanto, o proprietário do recurso pode conceder permissões de acesso a outros usuários e recursos. Uma maneira de fazer isso é escrever uma política de acesso.

Se AWS Config criar um bucket do Amazon S3 para você automaticamente (por exemplo, se você usar o AWS Config console para configurar seu canal de entrega), essas permissões serão adicionadas automaticamente ao bucket do Amazon S3. No entanto, se você especificar um bucket do S3 existente, garanta que esse bucket tenha as permissões corretas.

> **Note**
>
> Um objeto não herda as permissões de seu bucket. Por exemplo, se criar um bucket e conceder acesso de gravação a outro usuário, você não poderá acessar os objetos desse usuário, a menos que ele conceda o acesso explicitamente.

Sumário

- Permissões obrigatórias para o bucket do Amazon S3 ao usar perfis do IAM
- Permissões obrigatórias para o bucket do Amazon S3 ao usar perfis vinculados ao serviço
- Concedendo AWS Config acesso ao Amazon S3 Bucket

Permissões obrigatórias para o bucket do Amazon S3 ao usar perfis do IAM

Quando AWS Config envia informações de configuração (arquivos de histórico e snapshots) para o bucket do Amazon S3 em sua conta, ele assume a função do IAM que você atribuiu ao configurar. AWS Config Quando o AWS Config enviar informações de configuração para um bucket do S3 em outra conta, ele tentará usar o perfil do IAM. No entanto, essa tentativa falhará se a política de acesso do bucket não conceder acesso `WRITE` ao perfil do IAM. Nesse caso, AWS Config envia as informações novamente, desta vez como responsável pelo AWS Config serviço. Antes que a entrega seja bem-sucedida, a política de acesso deve conceder `WRITE` acesso ao nome `config.amazonaws.com` principal. AWS Config é então o proprietário dos objetos que ele entrega ao bucket do S3. Você deve associar uma política de acesso, mencionada na etapa 6 abaixo, ao bucket do S3 em outra conta para conceder ao AWS Config acesso ao bucket do S3.

Antes de AWS Config poder entregar registros para seu bucket do Amazon S3, AWS Config verifique se o bucket existe e em qual AWS região o bucket está localizado. AWS Config tenta chamar a

HeadBucketAPI do Amazon S3 para verificar se o bucket existe e obter a região do bucket. Se as permissões não forem fornecidas para localizar o bucket quando a verificação de localização for realizada, você verá `AccessDenied` um erro nos AWS CloudTrail registros. No entanto, a entrega de logs para o bucket do S3 será bem-sucedida se você não fornecer permissões para localização do bucket.

> **Note**
>
> Para fornecer permissão à API `HeadBucket` do Amazon S3, conceda permissão para realizar a ação `s3:ListBucket` como o Sid `AWSConfigBucketExistenceCheck`, mencionado na etapa 6 abaixo.

Permissões obrigatórias para o bucket do Amazon S3 ao usar perfis vinculados ao serviço

A função AWS Config vinculada ao serviço não tem permissão para colocar objetos nos buckets do Amazon S3. Portanto, se você configurar AWS Config usando uma função vinculada ao serviço, AWS Config enviará itens de configuração como principal do AWS Config serviço. Você precisará anexar uma política de acesso, mencionada na etapa 6 abaixo, ao bucket do Amazon S3 em sua própria conta ou em outra conta para conceder AWS Config acesso ao bucket do Amazon S3.

Concedendo AWS Config acesso ao Amazon S3 Bucket

Siga estas etapas para adicionar uma política de acesso a um bucket do S3 em sua própria conta ou em outra conta. A política de acesso permite AWS Config enviar informações de configuração para um bucket do Amazon S3.

1. Faça login no AWS Management Console usando a conta que tem o bucket do S3.
2. Abra o console do Amazon S3 em https://console.aws.amazon.com/s3/.
3. Selecione o bucket que você deseja usar AWS Config para entregar itens de configuração e, em seguida, escolha Propriedades.
4. Escolha Permissões.
5. Escolha Edit Bucket Policy (Editar política de bucket).
6. Copie a seguinte política na janela Bucket Policy Editor (Editor de políticas de bucket):

> **Important**
>
> Como melhor prática de segurança ao permitir o AWS Config acesso a um bucket do Amazon S3, recomendamos fortemente que você restrinja o acesso na política de bucket com a `AWS:SourceAccount` condição. Se sua política de bucket atual não seguir essa prática recomendada de segurança, recomendamos que você a edite para incluir essa proteção. Isso garante que o acesso AWS Config seja concedido somente em nome dos usuários esperados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
```

```
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

> **Note**
>
> Ao conceder permissões para sua função do IAM em vez do nome principal do AWS Config serviço (SPN), certifique-se de que sua função do IAM tenha `PutObjectACL` permissão no bucket entre contas para evitar erros de permissão insuficientes. Veja uma amostra de uma política de perfil do IAM em Política de perfil do IAM para o bucket do S3.

7. Substitua os seguintes valores na política do bucket:
   - *`target BucketName`* — O nome do bucket do Amazon S3 para o qual AWS Config entregará os itens de configuração.
   - *`[opcional] prefix`*: um acréscimo opcional à chave de objeto do S3 que ajuda a criar uma organização semelhante a pastas no bucket.
   - *`sourceAccountID`* — O ID da conta para a qual AWS Config entregará os itens de configuração ao bucket de destino.
8. Escolha Save (Salvar) e Close (Fechar).

Você pode usar a condição `AWS:SourceAccount` na política de bucket do Amazon S3 acima para restringir a entidade principal de serviço do Config para interagir somente com o bucket do S3

ao realizar operações em nome de contas específicas. Se você planeja configurar várias contas da mesma organização para entregar itens de configuração AWS Config em um único bucket do Amazon S3, recomendamos usar funções do IAM em vez de funções vinculadas ao serviço para que você possa usar chaves de AWS Organizations condições, como. `AWS:PrincipalOrgID` Para obter mais informações sobre o gerenciamento de permissões de acesso para usar com uma função do IAM AWS Config, consulte Permissões para a função do IAM atribuída AWS Config a. Para obter mais informações sobre como gerenciar permissões de acesso para AWS Organizations, consulte Gerenciando permissões de acesso para sua AWS organização.

AWS Config também suporta a `AWS:SourceArn` condição que restringe o principal do serviço Config a interagir apenas com o bucket do Amazon S3 ao realizar operações em nome de canais de entrega específicos. AWS Config Ao usar o principal de AWS Config serviço, a `AWS:SourceArn` propriedade sempre será definida como `arn:aws:config:sourceRegion:sourceAccountID:*` onde `sourceRegion` está a região do canal de entrega e `sourceAccountID` é a ID da conta que contém o canal de entrega. Para obter mais informações sobre canais AWS Config de entrega, consulte Gerenciando o canal de entrega. Por exemplo, adicione a seguinte condição para restringir a entidade principal de serviço do Config a interagir com seu bucket do Amazon S3 somente em nome de um canal de entrega na região `us-east-1` da conta `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Permissões para a chave KMS para o canal AWS Config de entrega

Use as informações deste tópico se quiser criar uma política para uma AWS KMS chave para seu bucket do S3 que permita usar a criptografia baseada em KMS em objetos entregues AWS Config para entrega do bucket do S3.

Sumário

- Permissões obrigatórias para a chave KMS ao usar perfis do IAM (entrega do bucket do S3)
- Permissões necessárias para a AWS KMS chave ao usar funções vinculadas ao serviço (S3 Bucket Delivery)
- Concedendo AWS Config acesso à chave AWS KMS

Permissões obrigatórias para a chave KMS ao usar perfis do IAM (entrega do bucket do S3)

Se você configurar AWS Config usando uma função do IAM, poderá anexar a seguinte política de permissão à chave KMS:

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> Se a função do IAM, a política de bucket do Amazon S3 ou a AWS KMS chave não fornecerem acesso adequado AWS Config, a tentativa AWS Config de enviar informações de configuração para o bucket do Amazon S3 falhará. Nesse caso, AWS Config envia as informações novamente, desta vez como responsável pelo AWS Config serviço. Nesse caso, você deve anexar uma política de permissão, mencionada abaixo, à AWS KMS chave para conceder AWS Config acesso ao uso da chave ao entregar informações ao bucket do Amazon S3.

Permissões necessárias para a AWS KMS chave ao usar funções vinculadas ao serviço (S3 Bucket Delivery)

A função AWS Config vinculada ao serviço não tem permissão para acessar a AWS KMS chave. Portanto, se você configurar AWS Config usando uma função vinculada ao serviço, AWS Config enviará informações como principal do AWS Config serviço. Você precisará anexar uma política de

acesso, mencionada abaixo, à AWS KMS chave para conceder AWS Config acesso ao uso da AWS KMS chave ao entregar informações ao bucket do Amazon S3.

Concedendo AWS Config acesso à chave AWS KMS

Essa política permite AWS Config usar uma AWS KMS chave ao entregar informações para um bucket do Amazon S3

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

Substitua os seguintes valores na política de chave:

- *`myKMSkeyARN`* — O ARN da chave usada para criptografar dados AWS KMS no bucket do Amazon S3 que entregará itens de configuração para o. AWS Config
- *`sourceAccountID`*: o ID da conta para a qual o AWS Config fornecerá os itens de configuração.

Você pode usar a `AWS:SourceAccount` condição na política de AWS KMS chaves acima para restringir o principal do serviço Config a interagir apenas com a AWS KMS chave ao realizar operações em nome de contas específicas.

AWS Config também suporta a `AWS:SourceArn` condição que restringe o principal do serviço Config a interagir apenas com o bucket do Amazon S3 ao realizar operações em nome de canais de entrega específicos. AWS Config Ao usar o principal de AWS Config serviço, a `AWS:SourceArn` propriedade sempre será definida como `arn:aws:config:sourceRegion:sourceAccountID:*` onde `sourceRegion` está a região do canal de entrega e `sourceAccountID` é a ID da conta que contém o canal de entrega. Para obter mais informações sobre canais AWS Config de entrega, consulte Gerenciando o canal de entrega. Por exemplo, adicione a seguinte condição para restringir a entidade principal de serviço do Config a interagir com seu bucket do Amazon S3 somente em nome de um canal de entrega na região `us-east-1` da conta `123456789012`: `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

Permissões para o tópico do Amazon SNS

Este tópico descreve como configurar AWS Config para entregar tópicos do Amazon SNS pertencentes a uma conta diferente. AWS Config deve ter as permissões necessárias para enviar notificações para um tópico do Amazon SNS. Para configurar a mesma conta, quando o AWS Config console cria um tópico do Amazon SNS ou você escolhe um tópico do Amazon SNS da sua própria conta AWS Config , certifique-se de que o tópico do Amazon SNS inclua as permissões necessárias e siga as melhores práticas de segurança.

> **Note**
>
> AWS Config atualmente oferece suporte somente ao acesso na mesma região e em todas as contas. Os tópicos do SNS usados para documentos de remediação AWS Systems Manager (SSM) ou para o canal de entrega do gravador não podem ser entre regiões.

Sumário

- Permissões obrigatórias para o tópico do Amazon SNS ao usar perfis do IAM
- Permissões obrigatórias para o tópico do Amazon SNS ao usar perfis vinculados ao serviço
- Concedendo AWS Config acesso ao tópico do Amazon SNS.
- Solução de problemas para um tópico do Amazon SNS

Permissões obrigatórias para o tópico do Amazon SNS ao usar perfis do IAM

Você pode associar uma política de permissões ao tópico do SNS de propriedade de uma conta diferente. Se você deseja usar um tópico do SNS de outra conta, anexe a política a seguir a um tópico existente do SNS.

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

Na chave `Resource`, *`account-id`* é o número da conta da AWS do proprietário do tópico. Para *`account-id1`*, *`account-id2 e account-id3`*, use o que Contas da AWS enviará dados para um tópico do Amazon SNS. Você pode substituir os valores adequados para *`region`* e *`myTopic`*.

Quando AWS Config envia uma notificação para um tópico do Amazon SNS, ele primeiro tenta usar a função do IAM, mas essa tentativa falha se a função ou Conta da AWS não tiver permissão para publicar no tópico. Nesse caso, AWS Config envia a notificação novamente, desta vez como um nome principal AWS Config de serviço (SPN). Para a publicação ser bem-sucedida, a política de acesso para o tópico deve conceder acesso `sns:Publish` ao nome de entidade principal `config.amazonaws.com`. Você deve anexar uma política de acesso, descrita na próxima seção, ao tópico do Amazon SNS para conceder ao AWS Config acesso ao tópico do SNS se o perfil do IAM não tiver permissão para publicar no tópico.

Permissões obrigatórias para o tópico do Amazon SNS ao usar perfis vinculados ao serviço

A função AWS Config vinculada ao serviço não tem permissão para acessar o tópico do Amazon SNS. Portanto, se você configurar AWS Config usando uma função vinculada ao serviço (SLR), AWS Config enviará informações como principal do AWS Config serviço. Você precisará anexar uma política de acesso, mencionada abaixo, ao tópico do Amazon SNS para conceder AWS Config acesso e enviar informações ao tópico do Amazon SNS.

Para a configuração da mesma conta, quando o tópico do Amazon SNS e o SLR estão na mesma conta e a política do Amazon SNS concede ao SLR a permissão “`sns:Publish`”, você não precisa usar o SPN do AWS Config . A política de permissões abaixo e as práticas recomendadas de segurança são para configuração entre contas.

Concedendo AWS Config acesso ao tópico do Amazon SNS.

Essa política permite AWS Config enviar uma notificação para um tópico do Amazon SNS. Para conceder AWS Config acesso ao tópico do Amazon SNS a partir de outra conta, você precisará anexar a seguinte política de permissões.

> **Note**
>
> Como prática recomendada de segurança, é altamente recomendável garantir AWS Config o acesso aos recursos em nome dos usuários esperados apenas restringindo o acesso às contas listadas na `AWS:SourceAccount` condição.

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
```

```
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

Na chave `Resource`, *`account-id`* é o número da conta da AWS do proprietário do tópico. Para *`account-id1`*, *`account-id2 e account-id3`*, use o que Contas da AWS enviará dados para um tópico do Amazon SNS. Você pode substituir os valores adequados para *`region`* e *`myTopic`*.

Você pode usar a `AWS:SourceAccount` condição na política de tópico anterior do Amazon SNS para restringir o nome principal do AWS Config serviço (SPN) para interagir somente com o tópico do Amazon SNS ao realizar operações em nome de contas específicas.

AWS Config também suporta a `AWS:SourceArn` condição que restringe o nome principal do AWS Config serviço (SPN) para interagir somente com o bucket do S3 ao realizar operações em nome de canais de entrega específicos AWS Config . Ao usar o nome principal do AWS Config serviço (SPN), a `AWS:SourceArn` propriedade sempre será definida como `arn:aws:config:sourceRegion:sourceAccountID:*` onde `sourceRegion` está a região do canal de entrega e `sourceAccountID` é a ID da conta que contém o canal de entrega. Para obter mais informações sobre canais AWS Config de entrega, consulte Gerenciando o canal de entrega. Por exemplo, adicione a seguinte condição para restringir o nome principal do AWS Config serviço (SPN) a interagir com seu bucket do S3 somente em nome de um canal de entrega na `us-east-1` região da conta`123456789012`:. `"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`

Solução de problemas para um tópico do Amazon SNS

AWS Config deve ter permissões para enviar notificações para um tópico do Amazon SNS. Se um tópico do Amazon SNS não puder receber notificações, verifique se a função do IAM que AWS Config estava assumindo tem as permissões necessárias. `sns:Publish`

Solução de problemas AWS Config de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Config um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Config
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Config recursos

Não estou autorizado a realizar uma ação em AWS Config

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para exibir detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `config:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 config:GetWidget on resource: my-example-widget
```

Nesse caso, a política de Mateo deve ser atualizada para permitir que ele tenha acesso ao recurso *`my-example-widget`* usando a ação `config:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Config.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Config. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS Config recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Config compatível com esses recursos, consulteComo AWS Config funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usando funções vinculadas ao serviço para AWS Config

AWS Config usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Config As funções vinculadas ao serviço são predefinidas AWS Config e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Config porque você não precisa adicionar manualmente as permissões necessárias. AWS Config define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Config pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para AWS Config

AWS Config usa a função vinculada ao serviço chamada AWSServiceRoleForConfig— AWS Config usa essa função vinculada ao serviço para chamar outros AWS serviços em seu nome.

A função AWSServiceRoleForConfigvinculada ao serviço confia no `config.amazonaws.com` serviço para assumir a função.

A política de permissões para a `AWSServiceRoleForConfig` função contém permissões somente leitura e somente gravação para recursos e permissões somente leitura para AWS Config recursos em outros serviços que oferecem suporte. AWS Config Para ver a política gerenciada AWSServiceRoleForConfig, consulte políticas AWS gerenciadas para AWS Config. Para ter mais informações, consulte Tipos de recursos compatíveis.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

Para usar uma função vinculada ao serviço com AWS Config, você deve configurar permissões em seu bucket do Amazon S3 e no tópico do Amazon SNS. Para obter mais informações, consulte Permissões obrigatórias para o bucket do Amazon S3 ao usar perfis vinculados ao serviço, Permissões necessárias para a AWS KMS chave ao usar funções vinculadas ao serviço (S3 Bucket

Delivery) e Permissões obrigatórias para o tópico do Amazon SNS ao usar perfis vinculados ao serviço.

Criando uma função vinculada ao serviço para AWS Config

Na CLI ou na API do IAM, crie uma função vinculada ao serviço com o nome de serviço `config.amazonaws.com`. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editando uma função vinculada ao serviço para AWS Config

AWS Config não permite que você edite a função AWSServiceRoleForConfigvinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para AWS Config

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

> **Note**
>
> Se o AWS Config serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir AWS Config recursos usados pelo AWSServiceRoleForConfig

Verifique se você não tem `ConfigurationRecorders` usando a função vinculada ao serviço. Você pode usar o AWS Config console para parar o gravador de configuração. Para interromper o registro, em Recording is on (Registro ativado), escolha Turn off (Desativar).

Você pode excluir o `ConfigurationRecorder` uso AWS Config da API. Para excluir, use o comando `delete-configuration-recorder`.

```
$ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM, a CLI do IAM ou a API do IAM para excluir a função vinculada ao AWSServiceRoleForConfig serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Resposta a incidentes em AWS Config

A segurança é a maior prioridade na AWS. Como parte do modelo de responsabilidade compartilhada AWS na nuvem, AWS gerencia uma arquitetura de data center, rede e software que atende aos requisitos das organizações mais sensíveis à segurança. AWS é responsável por qualquer resposta a incidentes com relação ao AWS Config serviço em si. Além disso, como AWS cliente, você compartilha a responsabilidade de manter a segurança na nuvem. Isso significa que você controla a segurança que escolhe implementar a partir das AWS ferramentas e recursos aos quais tem acesso e é responsável pela resposta a incidentes do seu lado do modelo de responsabilidade compartilhada.

Ao estabelecer um nível básico de segurança que atenda aos objetivos de seus aplicativos executados na nuvem, você pode detectar desvios aos quais pode reagir. Como a resposta a incidentes de segurança pode ser um tópico complexo, recomendamos que você analise os seguintes recursos para entender melhor o impacto que a resposta a incidentes (IR) e suas escolhas têm em suas metas corporativas: Guia de resposta a incidentes de AWS segurança, whitepaper de melhores práticas de AWS segurança e white paper sobre a perspectiva de segurança da estrutura de adoção de AWS nuvem (CAF).

Validação de conformidade para AWS Config

Auditores terceirizados avaliam a segurança e a conformidade AWS Config como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, FedRAMP, HIPAA e outros.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade

Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS Config

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenters tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança de infraestrutura em AWS Config

Como serviço gerenciado, AWS Config é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Config pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade

For AWS Config, AWS lida com tarefas básicas de segurança, como sistema operacional (SO) convidado e aplicação de patches em bancos de dados, configuração de firewall e recuperação de desastres.

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount`global `aws:SourceArn`e as chaves de contexto nas políticas de recursos para limitar as permissões que AWS Config concedem outro serviço ao recurso. Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou especificar vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curinga (`*`) para as partes desconhecidas do ARN. Por exemplo, .`arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`

Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves globais AWS Config para evitar o problema confuso do substituto: conceder AWS Config acesso ao Amazon S3 Bucket.

Melhores práticas de segurança para AWS Config

AWS Config fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

- Aproveite a marcação para AWS Config, que facilita o gerenciamento, a pesquisa e a filtragem de recursos.
- Confirme se seus canais de entrega foram configurados corretamente e, uma vez confirmados, verifique AWS Config se estão gravando corretamente.

Para obter mais informações, consulte o blog das Práticas recomendadas do AWS Config.

Registro e monitoramento em AWS Config

AWS Config é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS Config. O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS Config suas AWS soluções.

Tópicos

- Registrando chamadas de AWS Config API com AWS CloudTrail
- Monitorar

Registrando chamadas de AWS Config API com AWS CloudTrail

CloudTrail captura todas as chamadas de API AWS Config como eventos. As chamadas capturadas incluem chamadas do AWS Config console e chamadas de código para as operações AWS Config da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Config Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Config, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Tópicos

- AWS Config Informações em CloudTrail
- Compreendendo as entradas do arquivo de AWS Config log
- Exemplos de arquivos de registros

AWS Config Informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS Config, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no

seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua Conta da AWS, incluindo eventos para AWS Config, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas AWS Config as operações são registradas CloudTrail e documentadas na Referência da AWS Config API. Por exemplo, chamadas para as operações DeliverConfigSnapshot, DeleteDeliveryChannel e DescribeDeliveryChannels geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail UserIdentity.

Compreendendo as entradas do arquivo de AWS Config log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações

sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Exemplos de arquivos de registros

Para obter exemplos das entradas de CloudTrail registro, consulte os tópicos a seguir.

DeleteDeliveryChannel

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação DeleteDeliveryChannel.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação DeliverConfigSnapshot.

```
{
```

```
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```


DescribeConfigurationRecorderStatus

Veja a seguir um exemplo de arquivo de CloudTrail log da DescribeConfigurationRecorderStatusoperação.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação DescribeConfigurationGravadores.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
```

```
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação DescribeDeliveryChannels.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

Veja a seguir um exemplo de arquivo de CloudTrail log da GetResourceConfigHistoryoperação.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação do PutConfigurationGravador.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação PutDeliveryChannel.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação do StartConfigurationGravador.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

Veja a seguir um exemplo de arquivo de CloudTrail log para a operação do StopConfigurationGravador.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

Monitorar

Você pode usar outros AWS serviços para monitorar AWS Config recursos.

- Você pode usar o Amazon Simple Notification Service (SNS) para enviar notificações sempre que um AWS recurso compatível for criado, atualizado ou modificado como resultado da atividade da API do usuário.
- Você pode usar EventBridge a Amazon para detectar e reagir às mudanças no status dos AWS Config eventos.

Tópicos

- Monitorando mudanças AWS de recursos com o Amazon SQS
- Monitoramento AWS Config com a Amazon EventBridge

Monitorando mudanças AWS de recursos com o Amazon SQS

AWS Config usa o Amazon Simple Notification Service (SNS) para enviar notificações sempre que um AWS recurso compatível é criado, atualizado ou modificado como resultado da atividade da API do usuário. No entanto, você pode estar interessado em apenas algumas alterações de configuração de recurso. Por exemplo, você pode considerar essencial saber quando alguém modifica a configuração de um grupo de segurança, mas não precisa monitorar sempre que há uma alteração nas tags em suas instâncias do Amazon EC2. Ou, você pode fazer um programa que realiza ações específicas quando recursos específicos são atualizados. Por exemplo, você pode querer iniciar um determinado fluxo de trabalho quando uma configuração de um grupo de segurança é alterada. Se você quiser consumir programaticamente os dados dessas ou de AWS Config outras formas, use uma fila do Amazon Simple Queue Service como ponto final de notificação para o Amazon SNS.

> **Note**
>
> As notificações também podem vir do SNS na forma de e-mail, mensagem SMS (Short Message Service) para celulares e smartphones habitados para o serviço SMS, mensagem de notificação para um aplicativo em um dispositivo móvel ou mensagem de notificação para um ou mais endpoints HTTP ou HTTPS.

Você pode fazer com que uma única fila do SQS se inscreva em vários tópicos, independentemente de ter um tópico para cada região ou um tópico para cada conta de cada região. Você deve se inscrever na fila do tópico SNS desejado. (Você pode se inscrever em várias filas para um tópico SNS.) Para obter mais informações, consulte Enviar mensagens do Amazon SNS para filas do Amazon SQS.

Permissões para o Amazon SQS

Para usar o Amazon SQS com AWS Config, você deve configurar uma política que conceda permissões à sua conta para realizar todas as ações permitidas em uma fila do SQS. O exemplo de política a seguir concede permissão aos números de conta 111122223333 e 444455556666 para enviar mensagens pertencentes a cada alteração de configuração para a fila denominada arn:aws:sqs:us-east-2:444455556666:queue1.

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

Você também deve criar uma política que conceda permissões para conexões entre um tópico SNS e a fila SQS que se inscreve para aquele tópico. Veja a seguir um exemplo de política que permite que o tópico do SNS com o Amazon Resource Name (ARN) arn:aws:sns:us-east- 2:111122223333:test-topic execute qualquer ação na fila chamada arn:aws:sqs:us-east-2:111122223333:. test-topic-queue

> **Note**
>
> A conta para o tópico SNS e a fila SQS devem estar na mesma região.

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

Cada política pode incluir instruções que abrangem apenas uma única fila, não várias filas. Para informações sobre outras restrições nas políticas do SQS, consulte Informações especiais para políticas do Amazon SQS.

Monitoramento AWS Config com a Amazon EventBridge

A Amazon EventBridge fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. Use EventBridge a Amazon para detectar e reagir às mudanças no status dos AWS Config eventos.

Você pode criar uma regra que será executada sempre que houver uma transição de estado ou quando houver uma transição para um ou mais estados que sejam de interesse. Então, com base nas regras que você cria, a Amazon EventBridge invoca uma ou mais ações-alvo quando um evento corresponde aos valores que você especifica em uma regra. A depender do tipo de evento, convém enviar notificações, capturar informações, tomar medidas corretivas, iniciar eventos ou tomar outras ações.

Antes de criar regras de eventos para AWS Config, no entanto, você deve fazer o seguinte:

- Familiarize-se com eventos, regras e metas em EventBridge. Para obter mais informações, consulte O que é a Amazon EventBridge?
- Para obter mais informações sobre como começar EventBridge e configurar regras, consulte Introdução à Amazon EventBridge.
- Criar um ou mais destinos que você usará nas suas regras de evento.

Tópicos

- EventBridge Formato Amazon para AWS Config
- Criação de EventBridge regras da Amazon para AWS Config

EventBridge Formato Amazon para AWS Config

O EventBridge evento para AWS Config tem o seguinte formato:

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

Criação de EventBridge regras da Amazon para AWS Config

Use as etapas a seguir para criar uma EventBridge regra que é acionada em um evento emitido por. AWS Config Os eventos são emitidos com base no melhor esforço.

1. No painel de navegação, escolha Regras.
2. Escolha Create rule.

3. Insira um nome e uma descrição para a regra.

   Uma regra não pode ter o mesmo nome que outra na mesma Região e barramento de eventos.

4. Em Tipo de Regra, escolha Regra com Padrão de Evento.
5. Em Origem do evento, escolha AWS eventos ou eventos de EventBridge parceiros.
6. (Opcional) Para Exemplo de tipo evento, selecione Eventos da AWS .
7. (Opcional) Para Exemplo de eventos, escolha o tipo de evento que aciona a regra:
   - Escolha AWS API Call via CloudTrail para basear as regras nas chamadas de API feitas para esse serviço. Para obter mais informações sobre a criação desse tipo de regra, consulte Tutorial: Criar uma EventBridge regra da Amazon para chamadas de AWS CloudTrail API.
   - Escolha Config Configuration Item Change (Alteração de itens de configuração do Config) para receber notificações quando um recurso na sua conta for alterado.

     Conforme descrito nesses artigos de suporte, você pode usar EventBridge para receber notificações personalizadas por e-mail quando um recurso é criado ou excluído. Como posso receber notificações personalizadas por e-mail quando um recurso é criado no meu AWS Config serviço de Conta da AWS uso? e Como posso receber notificações personalizadas por e-mail quando um recurso é excluído do meu AWS Config serviço de Conta da AWS uso? .
   - Escolha Config Rules Compliance Change (Alteração da compatibilidade das regras do Config) para receber notificações quando uma verificação de conformidade para suas regras apresentar falha.

     Conforme descrito neste artigo de suporte, você pode usar EventBridge para receber notificações personalizadas por e-mail quando um recurso não está em conformidade. Como posso ser notificado quando um AWS recurso não está em conformidade usando? AWS Config.
   - Escolha Config Rules Re-evaluation Status (Status de reavaliação das regras do Config) para obter as notificações de status de reavaliação.
   - Escolha Config Configuration Snapshot Delivery Status (Status de entrega de snapshots da configuração do Config) para obter notificações de status de entrega de snapshot de configuração.
   - Escolha Config Configuration History Delivery Status (Status de entrega do histórico da configuração do Config) para obter notificações de status de entrega de histórico de configuração.
8. Em Método de criação, escolha Usar formulário de padrão.
9. Em Fonte do evento, selecione Serviços da AWS .

10. Em Serviço da AWS , escolha Config.
11. Em Tipo de evento, escolha o tipo de evento que aciona a regra:
    - Escolha Todos os eventos para criar uma regra que se aplique a todos os AWS serviços. Se você escolher essa opção, não poderá escolher tipos específicos de mensagens, nomes de regras, tipos de recursos ou IDs de recursos.
    - Escolha AWS API Call via CloudTrail para basear as regras nas chamadas de API feitas para esse serviço. Para obter mais informações sobre a criação desse tipo de regra, consulte Tutorial: Criar uma EventBridge regra da Amazon para chamadas de AWS CloudTrail API.
    - Escolha Config Configuration Item Change (Alteração de itens de configuração do Config) para receber notificações quando um recurso na sua conta for alterado.

      Conforme descrito nesses artigos de suporte, você pode usar EventBridge para receber notificações personalizadas por e-mail quando um recurso é criado ou excluído. Como posso receber notificações personalizadas por e-mail quando um recurso é criado no meu AWS Config serviço de Conta da AWS uso? e Como posso receber notificações personalizadas por e-mail quando um recurso é excluído do meu AWS Config serviço de Conta da AWS uso? .
    - Escolha Config Rules Compliance Change (Alteração da compatibilidade das regras do Config) para receber notificações quando uma verificação de conformidade para suas regras apresentar falha.

      Conforme descrito neste artigo de suporte, você pode usar EventBridge para receber notificações personalizadas por e-mail quando um recurso não está em conformidade. Como posso ser notificado quando um AWS recurso não está em conformidade usando? AWS Config.
    - Escolha Config Rules Re-evaluation Status (Status de reavaliação das regras do Config) para obter as notificações de status de reavaliação.
    - Escolha Config Configuration Snapshot Delivery Status (Status de entrega de snapshots da configuração do Config) para obter notificações de status de entrega de snapshot de configuração.
    - Escolha Config Configuration History Delivery Status (Status de entrega do histórico da configuração do Config) para obter notificações de status de entrega de histórico de configuração.
12. Escolha Any message type (Qualquer tipo de mensagem) para receber notificações de qualquer tipo. Escolha Specific message type(s) (Tipos de mensagem específica) para receber os seguintes tipos de notificações:

- Se você escolher ConfigurationItemChangeNotification, receberá mensagens quando a configuração de um recurso que AWS Config avalia for alterada.
- Se você escolher ComplianceChangeNotificação, receberá mensagens quando o tipo de conformidade de um recurso que AWS Config avalia for alterado.
- Se você escolher ConfigRulesEvaluationStarted, receberá mensagens quando AWS Config começar a avaliar sua regra em relação aos recursos especificados.
- Se você escolher ConfigurationSnapshotDeliveryCompleted, você receberá mensagens quando entregar AWS Config com sucesso o snapshot de configuração para seu bucket do Amazon S3.
- Se você escolher ConfigurationSnapshotDeliveryFailed, receberá mensagens quando AWS Config não conseguir entregar o snapshot de configuração ao seu bucket do Amazon S3.
- Se você escolher ConfigurationSnapshotDeliveryStarted, receberá mensagens quando AWS Config começar a entregar o snapshot de configuração para seu bucket do Amazon S3.
- Se você escolher ConfigurationHistoryDeliveryCompleted, você receberá mensagens quando entregar AWS Config com sucesso o histórico de configuração para seu bucket do Amazon S3.

13. Se você escolheu um tipo de evento específico na lista suspensa Tipo de evento, escolha Qualquer tipo de recurso para criar uma regra que se aplique a todos os tipos de recursos AWS Config compatíveis.

    Se preferir, pode escolher Specific resource type(s) (Tipos de recursos específicos). Em seguida, digite o tipo de recurso compatível com o AWS Config (por exemplo: `AWS::EC2::Instance`).

14. Se você escolheu um tipo de evento específico da lista suspensa Tipo de evento, escolha Qualquer ID de recurso para incluir algum ID de recurso compatível com o AWS Config .

    Se preferir, pode escolher Specific resource ID(s) (IDs de recursos específicos). Em seguida, digite o ID de recurso suportado pelo AWS Config (por exemplo: `i-04606de676e635647`).

15. Se você escolheu um tipo de evento específico da lista suspensa Tipo de evento, escolha Qualquer nome de regra para incluir alguma regra compatível com o AWS Config .

    Ou, escolha Specific rule name(s) (Nomes de regras específicas) e digite a regra compatível com o AWS Config (por exemplo: required-tags).

16. Em Selecionar destino(s), escolha o tipo de destino preparado para usar com essa regra e configure as opções adicionais necessárias a esse tipo.

17. Os campos exibidos variam de acordo com o serviço escolhido. Insira as informações específicas desse tipo de destino conforme necessário.

18. Para muitos tipos de alvo, EventBridge precisa de permissões para enviar eventos para o alvo. Nesses casos, EventBridge você pode criar a função do IAM necessária para que sua regra seja executada.
    - Para criar um perfil do IAM automaticamente, escolha Criar novo perfil para este recurso específico.
    - Para usar uma função do IAM que você criou anteriormente, escolha Use existing role (Usar função existente)
19. (Opcional) Selecione Add target (Adicionar destino) para adicionar outro destino a essa regra.
20. (Opcional) Insira uma ou mais tags para a regra. Para obter mais informações, consulte as EventBridge tags da Amazon.
21. Analise a configuração da regra para garantir que ela atenda aos requisitos de monitoramento de evento.
22. Escolha Criar regra para confirmar sua seleção.

Usando AWS Config com a interface Amazon VPC Endpoints

Se você usa a Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode estabelecer uma conexão privada entre sua VPC e. AWS Config Você pode usar essa conexão para se comunicar com o AWS Config a partir da VPC sem passar pela Internet pública.

O Amazon VPC é um AWS serviço que você pode usar para lançar AWS recursos em uma rede virtual que você define. Com a VPC, você tem controle sobre as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Os endpoints VPC da Interface são alimentados por AWS PrivateLink uma AWS tecnologia que permite a comunicação privada entre AWS serviços usando uma interface de rede elástica com endereços IP privados. Para conectar sua VPC a AWS Config, você define uma interface para a qual VPC endpoint. AWS Config Esse tipo de endpoint permite que você conecte sua VPC AWS aos serviços. O endpoint fornece conectividade confiável e escalável AWS Config sem a necessidade de um gateway de internet, instância de tradução de endereços de rede (NAT) ou conexão VPN. Para obter mais informações, consulte O que é a Amazon VPC? no Manual do usuário da Amazon VPC.

As etapas a seguir são para usuários da Amazon VPC. Para obter mais informações, consulte Conceitos básicos no Guia do usuário da Amazon VPC.

Crie um VPC Endpoint para AWS Config

Para começar a usar AWS Config com sua VPC, crie uma interface VPC endpoint para. AWS Config Você não precisa alterar as configurações do AWS Config. AWS Config chama outros AWS serviços usando seus endpoints públicos. Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Perguntas frequentes

Não consigo ver minhas últimas alterações de configuração

Posso esperar ver minhas alterações de configuração imediatamente?

AWS Config geralmente registra as alterações de configuração em seus recursos logo após a detecção de uma alteração ou na frequência especificada por você. No entanto, isso é feito com base no melhor esforço e às vezes pode levar mais tempo. Se os problemas persistirem depois de algum tempo, entre em contato AWS Supporte forneça suas AWS Config métricas que são suportadas pela Amazon. CloudWatch Para obter informações sobre essas métricas, consulte Métricas de AWS Config uso e sucesso.

Relações indiretas em AWS Config

Tópicos

- O que é relacionamento de recursos?
- O que é uma relação direta e indireta referente a um recurso?
- Quais relacionamentos indiretos AWS Config apoiam?
- Como os itens de configuração são criados devido ao relacionamento direto e indireto?
- Quais são os itens de configuração gerados devido a relacionamentos indiretos?
- Como faço para recuperar dados de configuração relacionados a relacionamentos indiretos?

O que é relacionamento de recursos?

Em AWS, recursos se referem a entidades que são gerenciáveis, como uma instância do Amazon Elastic Compute Cloud (Amazon EC2) AWS CloudFormation , uma pilha ou um bucket do Amazon S3. AWS Config é um serviço que rastreia e monitora recursos criando itens de configuração (CIs) sempre que uma alteração em um tipo de recurso registrado é detectada ou na frequência de gravação que você define. Por exemplo, quando AWS Config configurado para rastrear instâncias do Amazon EC2, ele cria um item de configuração toda vez que uma instância é criada, atualizada ou excluída. Cada item de configuração criado por AWS Config tem vários campos, incluindo`accountId`, `arn` (Amazon Resource Name) `awsRegionconfiguration`,`tags`,, `relationships` e. O campo de relacionamentos de um IC permite AWS Config exibir como os

recursos estão vinculados uns aos outros. Por exemplo, um relacionamento pode indicar que um volume do Amazon EBS com ID `vol-123ab45d` está vinculado a uma instância do Amazon EC2 com ID `i-a1b2c3d4`, que está associada ao grupo de segurança `sg-ef678hk`.

O que é uma relação direta e indireta referente a um recurso?

AWS Config deriva os relacionamentos da maioria dos tipos de recursos do campo de configuração, que são chamados de relacionamentos “diretos”. Um relacionamento direto é uma conexão unidirecional (A→B) entre um recurso (A) e outro recurso (B), normalmente obtida da descrição da resposta da API do recurso (A). No passado, para alguns tipos de recursos AWS Config inicialmente compatíveis, ele também capturava relacionamentos das configurações de outros recursos, criando relacionamentos “indiretos” que eram bidirecionais (B→A). Por exemplo, o relacionamento entre uma instância do Amazon EC2 e seu grupo de segurança é direta porque os grupos de segurança estão incluídos na resposta de descrição da API para a instância do Amazon EC2. Por outro lado, o relacionamento entre um grupo de segurança e uma instância do Amazon EC2 é indireta porque a descrição de um grupo de segurança não retorna nenhuma informação sobre as instâncias às quais ele está associado. Como resultado, quando é detectada uma alteração na configuração do recurso, o AWS Config não apenas cria um CI para esse recurso, mas também gera CIs para quaisquer recursos relacionados, incluindo aqueles com relacionamentos indiretos. Por exemplo, quando AWS Config detecta alterações em uma instância do Amazon EC2, ele cria um CI para a instância e um CI para o grupo de segurança associado à instância.

Quais relacionamentos indiretos AWS Config apoiam?

As seguintes relações indiretas de recursos são suportadas em AWS Config.

Tipo de recurso	está indiretamente relacionado ao tipo de recurso		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface` , `AWS::EC2::Subnet` , `AWS::EC2:`		

Tipo de recurso	está indiretamente relacionado ao tipo de recurso		
	`:VPNGateway` , `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` , `AWS::EC2::NetworkInterface`		
`AWS::EC2::Instance`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::NetworkInterface`	`AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::NetworkACL`	`AWS::EC2::Subnet` , `AWS::EC2::VPC`		
`AWS::EC2::VPNConnection`	`AWS::EC2::VPNGateway` , `AWS::EC2::CustomerGateway`		
`AWS::EC2::InternetGateway`	`AWS::EC2::VPC`		

Tipo de recurso	está indiretamente relacionado ao tipo de recurso		
`AWS::EC2::SecurityGroup`	`AWS::EC2::VPC`		
`AWS::EC2::Subnet`	`AWS::EC2::VPC`		
`AWS::EC2::VPNGateway`	`AWS::EC2::VPC`		

Como os itens de configuração são criados devido ao relacionamento direto e indireto?

Para um relacionamento direto entre recursos (A→B), qualquer alteração na configuração do recurso B também iniciará um item de configuração (CI) para o recurso A. Da mesma forma, para um relacionamento indireto (B→A), quando houver uma alteração na configuração do recurso A, um novo CI será gerado para o recurso B. Por exemplo, a instância do Amazon EC2 com o grupo de segurança é um relacionamento direto, portanto, qualquer alteração na configuração de um grupo de segurança geraria um CI para o grupo de segurança, bem como um CI para a instância do EC2. Da mesma forma, o grupo de segurança com a instância do Amazon EC2 é um relacionamento indireto, portanto, qualquer alteração na configuração de uma instância do EC2 geraria um CI para a instância do Amazon EC2, bem como um CI para o grupo de segurança.

Quais são os itens de configuração gerados devido a relacionamentos indiretos?

Abaixo estão os itens de configuração (CIs) adicionais gerados devido aos relacionamentos indiretos de recursos.

As alterações de configuração para os seguintes tipos de recursos	irá gerar CIs para os seguintes tipos e recursos		
AWS::EC2::RouteTable	AWS::EC2::Instance , AWS::EC2::NetworkInterface , AWS::EC2::Subnet , AWS::EC2::VPNGateway , e AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance , AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		

As alterações de configuração para os seguintes tipos de recursos	irá gerar CIs para os seguintes tipos e recursos		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway , AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

Como faço para recuperar dados de configuração relacionados a relacionamentos indiretos?

Você pode executar consultas SQL (Structured Query Language) em Consultas AWS Config avançadas para recuperar dados de configuração relacionados a relacionamentos indiretos de recursos. Por exemplo, se você quiser recuperar a lista de instâncias do Amazon EC2 relacionadas a um grupo de segurança, use a seguinte consulta:

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
```

```
    relationships.resourceId = 'sg-234213'
```

Exemplos de código para AWS Config usar AWS SDKs

Os exemplos de código a seguir mostram como usar AWS Config com um kit AWS de desenvolvimento de software (SDK).

Ações são trechos de código de programas maiores e devem ser executadas em contexto. Embora as ações mostrem como chamar funções de serviço específicas, é possível ver as ações contextualizadas em seus devidos cenários e exemplos entre serviços.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Exemplos de código

- Ações para AWS Config usar AWS SDKs
  - Use DeleteConfigRule com um AWS SDK ou CLI
  - Use DescribeComplianceByConfigRule com um AWS SDK ou CLI
  - Use DescribeComplianceByResource com um AWS SDK ou CLI
  - Use DescribeConfigRuleEvaluationStatus com um AWS SDK ou CLI
  - Use DescribeConfigRules com um AWS SDK ou CLI
  - Use DescribeConfigurationRecorderStatus com um AWS SDK ou CLI
  - Use DescribeConfigurationRecorders com um AWS SDK ou CLI
  - Use DescribeDeliveryChannels com um AWS SDK ou CLI
  - Use GetComplianceDetailsByConfigRule com um AWS SDK ou CLI
  - Use GetComplianceDetailsByResource com um AWS SDK ou CLI
  - Use GetComplianceSummaryByConfigRule com um AWS SDK ou CLI
  - Use GetComplianceSummaryByResourceType com um AWS SDK ou CLI
  - Use PutConfigRule com um AWS SDK ou CLI
  - Use PutDeliveryChannel com um AWS SDK ou CLI

Ações para AWS Config usar AWS SDKs

Os exemplos de código a seguir demonstram como realizar AWS Config ações individuais com AWS SDKs. Esses trechos chamam a AWS Config API e são trechos de código de programas maiores

que devem ser executados em contexto. Cada exemplo inclui um link para GitHub, onde você pode encontrar instruções para configurar e executar o código.

Os exemplos a seguir incluem apenas as ações mais utilizadas. Para obter uma lista completa, consulte a Referência de APIs do AWS Config.

Exemplos

- Use DeleteConfigRule com um AWS SDK ou CLI
- Use DescribeComplianceByConfigRule com um AWS SDK ou CLI
- Use DescribeComplianceByResource com um AWS SDK ou CLI
- Use DescribeConfigRuleEvaluationStatus com um AWS SDK ou CLI
- Use DescribeConfigRules com um AWS SDK ou CLI
- Use DescribeConfigurationRecorderStatus com um AWS SDK ou CLI
- Use DescribeConfigurationRecorders com um AWS SDK ou CLI
- Use DescribeDeliveryChannels com um AWS SDK ou CLI
- Use GetComplianceDetailsByConfigRule com um AWS SDK ou CLI
- Use GetComplianceDetailsByResource com um AWS SDK ou CLI
- Use GetComplianceSummaryByConfigRule com um AWS SDK ou CLI
- Use GetComplianceSummaryByResourceType com um AWS SDK ou CLI
- Use PutConfigRule com um AWS SDK ou CLI
- Use PutDeliveryChannel com um AWS SDK ou CLI

Use **`DeleteConfigRule`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DeleteConfigRule`.

CLI

AWS CLI

Para excluir uma regra de AWS Config

O comando a seguir exclui uma regra de AWS Config chamada: `MyConfigRule`

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- Para obter detalhes da API, consulte DeleteConfigRuleem Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3).

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- Para obter detalhes da API, consulte a DeleteConfigRuleReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeComplianceByConfigRule`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeComplianceByConfigRule`.

CLI

AWS CLI

Para obter informações de conformidade para suas regras de AWS Config

O comando a seguir retorna informações de conformidade para cada regra AWS do Config violada por um ou mais recursos: AWS

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos não estão em conformidade com a regra relacionada. Por exemplo, a saída a seguir indica que três recursos não estão em conformidade com a regra nomeada`InstanceTypesAreT2micro`.

Saída:

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
```

```
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeComplianceByConfigRuleem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo recupera detalhes de conformidade da regra ebs-optimized-instance, para os quais não há resultados de avaliação atuais para a regra, portanto, retorna INSUFFICIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

Saída:

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

Exemplo 2: Esse exemplo retorna o número de recursos não compatíveis para a regra ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK.

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

Saída:

```
CapExceeded CappedCount
----------- -----------
False       2
```

- Para obter detalhes da API, consulte DescribeComplianceByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use `DescribeComplianceByResource` com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeComplianceByResource`.

CLI

AWS CLI

Para obter informações de conformidade para seus AWS recursos

O comando a seguir retorna informações de conformidade para cada instância do EC2 que é registrada pelo AWS Config e que viola uma ou mais regras:

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

Na saída, o valor de cada `CappedCount` atributo indica quantas regras o recurso viola. Por exemplo, a saída a seguir indica que a instância `i-1a2b3c4d` viola duas regras.

Saída:

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
```

```
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeComplianceByResourceem Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo verifica o tipo **`AWS::SSM::ManagedInstanceInventory`** de recurso quanto ao tipo de conformidade “COMPATÍVEL”.

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

Saída:

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- Para obter detalhes da API, consulte DescribeComplianceByResourceem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeConfigRuleEvaluationStatus`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeConfigRuleEvaluationStatus`.

CLI

AWS CLI

Para obter informações de status de uma regra AWS Config

O comando a seguir retorna as informações de status de uma regra AWS Config chamada: `MyConfigRule`

```
aws configservice describe-config-rule-evaluation-status --config-rule-names
 MyConfigRule
```

Saída:

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeConfigRuleEvaluationStatusna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna as informações de status das regras de configuração fornecidas.

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

Saída:

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- Para obter detalhes da API, consulte DescribeConfigRuleEvaluationStatusem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulte Usando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeConfigRules`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeConfigRules`.

CLI

AWS CLI

Para obter detalhes de uma regra AWS Config

O comando a seguir retorna detalhes de uma regra de AWS Config chamada: `InstanceTypesAreT2micro`

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

Saída:

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
```

```
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeConfigRulesna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo lista as regras de configuração da conta, com propriedades selecionadas.

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

Saída:

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- Para obter detalhes da API, consulte DescribeConfigRulesem Referência de AWS Tools for PowerShell cmdlet.

Python

SDK para Python (Boto3).

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
```

```
        else:
            return rule
```

- Para obter detalhes da API, consulte a DescribeConfigRulesReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeConfigurationRecorderStatus`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeConfigurationRecorderStatus`.

CLI

AWS CLI

Para obter informações de status do gravador de configuração

O comando a seguir retorna o status do gravador de configuração padrão:

```
aws configservice describe-configuration-recorder-status
```

Saída:

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
```

```
}
```

- Para obter detalhes da API, consulte DescribeConfigurationRecorderStatusna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna o status dos gravadores de configuração.

```
Get-CFGConfigurationRecorderStatus
```

Saída:

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- Para obter detalhes da API, consulte DescribeConfigurationRecorderStatusem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeConfigurationRecorders`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeConfigurationRecorders`.

CLI

AWS CLI

Para obter detalhes sobre o gravador de configuração

O comando a seguir retorna detalhes sobre o gravador de configuração padrão:

```
aws configservice describe-configuration-recorders
```

Saída:

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeConfigurationRecordersna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo retorna os detalhes dos gravadores de configuração.

```
Get-CFGConfigurationRecorder | Format-List
```

Saída:

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- Para obter detalhes da API, consulte DescribeConfigurationRecordersem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`DescribeDeliveryChannels`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `DescribeDeliveryChannels`.

CLI

AWS CLI

Para obter detalhes sobre o canal de entrega

O comando a seguir retorna detalhes sobre o canal de entrega:

```
aws configservice describe-delivery-channels
```

Saída:

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- Para obter detalhes da API, consulte DescribeDeliveryChannelsna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo recupera o canal de entrega da região e exibe detalhes.

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

Saída:

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- Para obter detalhes da API, consulte DescribeDeliveryChannelsem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetComplianceDetailsByConfigRule`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetComplianceDetailsByConfigRule`.

CLI

AWS CLI

Para obter os resultados da avaliação de uma regra AWS Config

O comando a seguir retorna os resultados da avaliação de todos os recursos que não estão em conformidade com uma regra de AWS Config chamada: `InstanceTypesAreT2micro`

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

Saída:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
```

```
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceDetailsByConfigRulena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo obtém os resultados da avaliação da regra access-keys-rotated e retorna a saída agrupada por tipo de conformidade

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

Saída:

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

Exemplo 2: Este exemplo consulta os detalhes de conformidade da regra access-keys-rotated para recursos COMPATÍVEIS.

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

Saída:

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- Para obter detalhes da API, consulte GetComplianceDetailsByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **GetComplianceDetailsByResource** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetComplianceDetailsByResource`.

CLI

AWS CLI

Para obter os resultados da avaliação de um AWS recurso

O comando a seguir retorna os resultados da avaliação de cada regra com a qual a instância do EC2 `i-1a2b3c4d` não está em conformidade:

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

Saída:

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
```

```
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceDetailsByResourcena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Este exemplo de resultados de avaliação para o recurso fornecido.

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

Saída:

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- Para obter detalhes da API, consulte GetComplianceDetailsByResourceem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetComplianceSummaryByConfigRule`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetComplianceSummaryByConfigRule`.

CLI

AWS CLI

Para obter o resumo de conformidade de suas regras de AWS Config

O comando a seguir retorna o número de regras que estão em conformidade e o número que não estão em conformidade:

```
aws configservice get-compliance-summary-by-config-rule
```

Na saída, o valor de cada `CappedCount` atributo indica quantas regras estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByConfigRulena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna o número de regras do Config que não estão em conformidade.

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

Saída:

```
CapExceeded CappedCount
----------- -----------
False       9
```

- Para obter detalhes da API, consulte GetComplianceSummaryByConfigRuleem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`GetComplianceSummaryByResourceType`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `GetComplianceSummaryByResourceType`.

CLI

AWS CLI

Para obter o resumo de conformidade de todos os tipos de recursos

O comando a seguir retorna o número de AWS recursos que não estão em conformidade e o número que estão em conformidade:

```
aws configservice get-compliance-summary-by-resource-type
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummariesByResourceType": [
```

```
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

Para obter o resumo de conformidade de um tipo específico de recurso

O comando a seguir retorna o número de instâncias do EC2 que não estão em conformidade e o número que estão em conformidade:

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

Na saída, o valor de cada `CappedCount` atributo indica quantos recursos estão em conformidade ou não.

Saída:

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
```

```
                }
            }
        }
    ]
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByResourceTypena Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo retorna o número de recursos compatíveis ou não compatíveis e converte a saída em json.

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- Para obter detalhes da API, consulte GetComplianceSummaryByResourceTypeem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`PutConfigRule`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `PutConfigRule`.

CLI

AWS CLI

Para adicionar uma regra de Config AWS gerenciada

O comando a seguir fornece código JSON para adicionar uma regra Config AWS gerenciada:

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` é um arquivo JSON que contém a configuração da regra:

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

Para o `ComplianceResourceTypes` atributo, esse código JSON limita o escopo a recursos do `AWS::EC2::Instance` tipo, então o AWS Config avaliará somente instâncias do EC2 em relação à regra. Como a regra é uma regra gerenciada, o atributo `Owner` é definido como `AWS` e o atributo `SourceIdentifier` é definido como o identificador da regra, `REQUIRED_TAGS`. Para o atributo `InputParameters`, as chaves de tag exigidas pela regra, `CostCenter` e `Owner` são especificados.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar a configuração da regra, execute o describe-config-rules comando e especifique o nome da regra.

Como adicionar uma regra do Config gerenciada pelo cliente

O seguinte comando fornece o código JSON para adicionar uma regra do Config gerenciada pelo cliente:

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` é um arquivo JSON que contém a configuração da regra:

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

Para o `ComplianceResourceTypes` atributo, esse código JSON limita o escopo a recursos do `AWS::EC2::Instance` tipo, então o AWS Config avaliará somente instâncias do EC2 em relação à regra. Como essa regra é uma regra gerenciada pelo cliente, o `Owner` atributo é definido como`CUSTOM_LAMBDA`, e o `SourceIdentifier` atributo é definido como o ARN da função Lambda AWS . O `SourceDetails` objeto é obrigatório. Os parâmetros especificados para o `InputParameters` atributo são passados para a função AWS Lambda quando o AWS Config a invoca para avaliar os recursos em relação à regra.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar a configuração da regra, execute o describe-config-rules comando e especifique o nome da regra.

- Para obter detalhes da API, consulte PutConfigRulena Referência de AWS CLI Comandos.

Python

SDK para Python (Boto3).

> **Note**
>
> Tem mais sobre GitHub. Encontre o exemplo completo e veja como configurar e executar no AWS Code Examples Repository.

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
```

```
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- Para obter detalhes da API, consulte a PutConfigRuleReferência da API AWS SDK for Python (Boto3).

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Use **`PutDeliveryChannel`** com um AWS SDK ou CLI

Os exemplos de códigos a seguir mostram como usar `PutDeliveryChannel`.

CLI

AWS CLI

Para criar um canal de entrega

O comando a seguir fornece as configurações do canal de entrega como código JSON:

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

O `deliveryChannel.json` arquivo especifica os atributos do canal de entrega:

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

Esse exemplo define os seguintes atributos:

`name`- O nome do canal de entrega. Por padrão, o AWS Config atribui o nome `default` a um novo canal de entrega. Você não pode atualizar o nome do canal de entrega com o comando. `put-delivery-channel` Para ver as etapas para alterar o nome, consulte Renomear o canal de entrega. `s3BucketName` - O nome do bucket do Amazon S3 para o qual o AWS Config entrega snapshots de configuração e arquivos de histórico de configuração. Se você especificar um bucket que pertença a outra AWS conta, esse bucket deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para buckets do Amazon S3.

`snsTopicARN`- O Amazon Resource Name (ARN) do tópico do Amazon SNS para o qual o AWS Config envia notificações sobre alterações na configuração. Se você escolher um tópico de outra conta, o tópico deve ter políticas que concedam permissões de acesso ao Config. AWS Para obter mais informações, consulte Permissões para o tópico do Amazon SNS.

`configSnapshotDeliveryProperties`- Contém o `deliveryFrequency` atributo, que define com que frequência o AWS Config fornece instantâneos de configuração e com que frequência ele invoca avaliações para regras periódicas do Config.

Se o comando for bem-sucedido, o AWS Config não retornará nenhuma saída. Para verificar as configurações do seu canal de entrega, execute o describe-delivery-channels comando.

- Para obter detalhes da API, consulte PutDeliveryChannelna Referência de AWS CLI Comandos.

PowerShell

Ferramentas para PowerShell

Exemplo 1: Esse exemplo altera a propriedade deliveryFrequency de um canal de entrega existente.

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- Para obter detalhes da API, consulte PutDeliveryChannelem Referência de AWS Tools for PowerShell cmdlet.

Para obter uma lista completa dos guias do desenvolvedor do AWS SDK e exemplos de código, consulteUsando AWS Config com um AWS SDK. Este tópico também inclui informações sobre como começar e detalhes sobre versões anteriores do SDK.

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação do AWS Config. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

- Versão da API: 12/11/2014
- Última atualização da documentação: 17 de junho de 2024

Alteração	Descrição	Data
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para o Amazon Elastic File System (Amazon EFS), Amazon Redshift e. AWS Systems Manager para SAP Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	17 de junho de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • cloudtrail-s3-bucket-public-access proibido • registro de acesso ao bucket do cloudtrail-s3-	8 de maio de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte à seguinte	2 de maio de 2024

	regra gerenciada: iam-external-access-analyzer-enabled	
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • proteção contra malware guardduty-habilitada • proteção guardduty-rds-habilitada • proteção guardduty-s3 ativada • habilitado para escaneamento padrão inspetor-lambda	26 de abril de 2024
AWS Config simplifica a análise de uso com a Amazon CloudWatch	Com esta versão, as CloudWatch métricas da Amazon para monitorar o uso de AWS Config dados exibirão somente o uso faturável. Isso significa que o uso não faturável não será mais exibido nas CloudWatch métricas da Amazon emitidas para o console e para AWS Config o console. AWS Config Isso permite que você valide a AWS Config configuração e o uso usando as CloudWatch métricas da Amazon e correlacione o uso faturável com os custos associados. Para obter mais informações, consulte Métricas de AWS Config uso e sucesso.	26 de abril de 2024

AWS Config atualiza as regras gerenciadas	Com esta versão, é AWS Config compatível com a seguinte regra gerenciada: iam-server-certificate-expiration-check	23 de abril de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • verificação de restrição de porta vpc-sg- • cloudtrail-all-write-s3-data-event-check • verificação de eventos de dados cloudtrail-all-read-s3-	17 de abril de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • guardduty-eks-protection-audit-habilitado • guardduty-eks-protection-runtime-habilitado • habilitado para proteção guardduty-lambda • inspetor-ec2-scan habilitado • habilitado para inspector-ecr-scan • habilitado para escaneamento de código lambda do inspetor • redshift - acesso irrestrito à porta	16 de abril de 2024

AWS Config atualiza as regras gerenciadas	Com esta versão, é AWS Config compatível com a seguinte regra gerenciada: efs-mount-target-public-accessible	20 de março de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • dms-neptune-iam com autorização habilitada • habilitado para autenticação dms-mongo-db • habilitado para dms-redis-tls • criptografia de endpoint dax-tls- • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream criptografado • mq-cloudwatch-audit-log-habilitado • mq-cloudwatch-audit-log-habilitado • opensearch-primary-node-fault-tolerance • sagemaker-endpoint-config-prod-instance-count • catálogo de serviços compartilhado dentro da organização • transfer-family-server-no-ftp	26 de fevereiro de 2024

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para o Amazon Managed Service para Prometheus, CloudWatch Amazon, Amazon Cognito, Amazon, Amazon AWS Glue FSx ElastiCache,, (IAM) AWS Identity and Access Management ,,, Amazon Redshift Serverless AWS Lambda, AWS RAM Amazon e Amazon SageMaker Simple Notification Service (Amazon SNS). Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	22 de fevereiro de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte à seguinte regra gerenciada: s3-bucket-cross-region-replication-enabled	12 de fevereiro de 2024

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de recursos AWS AppConfig , Amazon CloudWatch Evidently AWS Identity and Access Management (IAM), Amazon MemoryDB for Redis (MemoryDB), Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Redshift e outros tipos de recursos. AWS Transfer Family Para obter mais informações, consulte Tipos de Recursos Compatíveis.	6 de fevereiro de 2024
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte à seguinte regra gerenciada: macie-auto-sensitive-data-discovery-check	29 de janeiro de 2024

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos Amazon AppStream, AWS Key Management Service (AWS KMS), Amazon Relational Database Service (Amazon RDS), Amazon Cognito, Amazon Elastic Compute Cloud (Amazon EC2), EC2 Image Builder AWS Ground Station,,, Amazon AWS Mainframe Modernization, Amazon Redshift e tipos de recursos. QuickSight AWS Systems Manager Para obter mais informações, consulte Tipos de Recursos Compatíveis.	3 de janeiro de 2024

Os limites de serviço aumentam para o número máximo de AWS Config regras por região por conta	Com esta versão, AWS Config suporta 1000 AWS Config regras por AWS região por conta. Esse aumento se aplica ao total de todas as regras implantadas, incluindo regras AWS Config gerenciadas, regras AWS Config personali zadas, pacotes de AWS Config conformidade, AWS Security Hub controles, AWS Firewall Manager políticas e planos de AWS Backup backup por região e por conta. Para obter mais informações, consulte Limites de serviço da .	19 de dezembro de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	19 de dezembro de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS AppConfig Amazon Managed Service for Prometheus AWS Database Migration Service ,AWS DMS(), () IAM,AWS Identity and Access Management Amazon Managed Streaming for Apache Kafka (Amazon MSK CloudWatch), Amazon Logs e Amazon Simple Storage Service (AWS Organizations Amazon S3). Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	5 de dezembro de 2023

Versão de pré-visualização: processador de consultas em linguagem natural para consultas avançadas	Com esta versão, você pode usar o processador de consulta de linguagem natural para consultas avançadas, que usa recursos de inteligência artificial generativa (IA generativa) que permitem fazer perguntas em inglês simples e convertê-las em um ready-to-use formato de consulta. Com o processador de consulta de linguagem natural, você pode consultar sua organização Conta da AWS ou em toda a AWS organização. Para obter mais informações, consulte Natural language query processor for advanced queries.	26 de novembro de 2023

Gravação periódica	Com esta versão, AWS Config suporta gravação periódica. A gravação periódica oferece a capacidade de capturar as alterações mais recentes na configuração dos recursos em um período fixo. Agora é possível definir a frequênci a padrão do gravador de configuração como Diária, permitindo receber um item de configuração (CI) que represente o estado mais recente dos recursos no último período de 24 horas, somente se for diferente do CI anterior gravado. O AWS Config console também apresenta uma nova experiênc ia de estratégia de gravação, na qual você também pode substituir a frequência de gravação por tipos de recursos específicos ou excluir tipos específicos de recursos da gravação. Isso pode ajudar a ajustar as configurações aos requisitos granulares. Os seguintes tipos de dados foram adicionados: • RecordingMode • RecordingModeSubstituir	26 de novembro de 2023

Os seguintes tipos de dados foram atualizados:

- PutConfigurationGravador
- ConfigurationRecorder
- BaseConfigurationItem
- ConfigurationItem

As seguintes páginas do guia do desenvolvedor foram atualizadas:

- Recursos de recodificação AWS
- Configuração AWS Config com o AWS Config console | Configuração com 1 clique
- Configuração AWS Config com o AWS Config console | Configuração manual
- Configurando AWS Config com a AWS CLI

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Cognito, Amazon Connect, Amazon EMR,, AWS Ground Station, AWS Mainframe Modernization Amazon MemoryDB for Redis, Amazon, QuickSight Amazon AWS Organizations Relational Database Service (Amazon RDS), Amazon Redshift, Amazon Route 53 e. AWS Service Catalog AWS Transfer Family Agora, as políticas `AWSConfigServiceRolePolicy` e `AWS_ConfigRole` também adicionam identificadores de segurança (SID) para as políticas `AWSConfigServiceRolePolicyStatementID` , `AWSConfigSLRLogStatementID` , `AWSConfigSLRLogEventStatementID` , `AWSConfigSLRApiGatewayStatementID` e `AWSConfigServiceRolePolicy` . Para obter mais informações, consulte AWS Políticas	17 de novembro de 2023

	gerenciadas para o AWS Config.	
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	9 de novembro de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em new AWS Identity and Access Management (IAM),, (), Amazon Connect AWS Network Manager, Amazon Elastic Compute Cloud AWS Private Certificate Authority (Amazon EC2 AWS Private CA), Amazon Elastic Container Service (Amazon ECS) Elastic Container Service (Amazon ECS),,, Amazon AWS IoT Managed Streaming AWS IoT TwinMaker for Apache Kafka Connect (Amazon MSK Connect Connect) e tipos de recursos. AWS App Mesh AWS Lambda Explorador de recursos da AWS Para obter mais informações, consulte Tipos de recursos compatíveis.	3 de novembro de 2023
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza o seguinte pacote de conformidade: Melhores práticas operacionais para BNM RMit	26 de outubro de 2023

Painéis de conformidade e inventário para agregadores	Com esta versão, AWS Config adiciona uma página de painel de conformidade e uma página de painel de inventário à exibição agregada no AWS Config console. Na página do painel de conformidade, você pode visualizar painéis automatiz ados com widgets que resumem os insights sobre a conformidade de recursos em seu agregador, como os 10 principais tipos de recursos por recursos não compatíve is, os 10 principais pacotes de conformidade em nível de conta por regras não compatíveis e muito mais. Para a página do painel de inventário, você pode visualiza r o painel automatizado com widgets que resumem os insights sobre os dados de configuração de recursos em seu agregador, como os 10 principais tipos de recursos por contagem de recursos, as 10 principais contas por contagem de recursos e muito mais. Para obter informações sobre gráficos e tabelas, consulte	23 de outubro de 2023

	Painel de conformidade e Painel de inventário.	
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS Private CA,, Amazon Connect AWS App Mesh, Amazon Elastic Container Service (Amazon ECS), Amazon Evidently, CloudWatch Amazon Managed Grafana, Amazon, Amazon AWS IoT Inspector GuardDuty,,, Amazon Managed Streaming for Apache Kafka (Amazon MSK) AWS IoT TwinMaker ,,,, e Amazon. AWS Lambda AWS Network Manager AWS Organizations SageMaker Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	4 de outubro de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de AWS IoT recursos AWS IoT TwinMaker, AWS IoT Wireless,, Amazon Personalize Amazon Managed Streaming for Apache Kafka (Amazon MSK) SageMaker , Amazon, AWS CodeBuild Amazon e Amazon AppStream Inspector. Para obter mais informações, consulte Tipos de recursos compatíveis.	4 de outubro de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled	21 de setembro de 2023

	• wafv2-rulegroup-logging-enabled • msk-in-cluster-node-require-tls	
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for Amazon S3 • Operational Best Practices for EC2	8 de setembro de 2023
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política agora remove as permissões para AWS Systems Manager (Systems Manager). Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	6 de setembro de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo Amazon CodeGuru Profiler,, AWS Elemental MediaConnect AWS Transfer Family, Amazon Managed Service for Prometheus, AWS Batch, AWS Cloud Map, e nos tipos de recursos. Amazon Route 53 Resolver Para obter mais informações, consulte Tipos de recursos compatíveis.	6 de setembro de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	10 de agosto de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos AWS Amplify, Amazon, Amazon Athena AppIntegrations AWS App Mesh, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently CloudWatch , Amazon Forecast,,,,,, Amazon Managed AWS Elemental MediaConvert Streaming AWS Elemental MediaTailor for Apache Kafka (Amazon MSK) AWS IoT Greengrass Version 2 AWS Ground Station, Amazon Personalize, Amazon Pinpoint Amazon Pinpoint e tipos de recursos. AWS Resilience Hub Para obter mais informações, consulte Tipos de recursos compatíveis.	3 de agosto de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Managed Workflows for Amazon AppStream 2.0 AWS App Mesh, Amazon,, Amazon Connect, Amazon AWS CloudFormation, AWS Identity and Access Management (IAM) CloudFront AWS CodeArtifact AWS CodeBuild, Amazon Inspector AWS Glue,, GuardDuty,, Amazon Managed Streaming for Apache Kafka AWS IoT, Amazon AWS Network Manager Explorador de recursos da AWS Macie AWS IoT TwinMaker AWS IoT Wireless,,,,,, Amazon Route 53, AWS Elemental MediaConnect Amazon Simple Storage Service (Amazon S3) Service S3), AWS Organizations Amazon Simple Notification Service (Amazon SNS), Simple Notification Service (Amazon SNS) e Amazon EC2 Systems Gerente (SSM). Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	28 de julho de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo Amazon Kinesis, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Pinpoint, Amazon Simple Storage Service (Amazon S3) Storage Service (Amazon S3), Amazon Virtual Private Cloud (Amazon VPC), Amazon Kendra, Amazon Connect Tipos de recursos Amazon Connect,, ,, e (). AWS CloudFormation AWS AppConfig AWS App Mesh AWS App Runner AWS Database Migration Service AWS DMS Para obter mais informações, consulte Tipos de recursos compatíveis.	10 de julho de 2023
Aumento dos limites de serviço para pacotes de conformidade organizacional	Com esta versão, AWS Config suporta 350 AWS Config regras por região por conta em todos os pacotes de conformidade e 350 AWS Config regras organizacionais por organização. Para obter mais informações, consulte Limites de serviço.	13 de junho de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Managed Workflows para Amazon Connect AWS Amplify, Amazon Managed Service for Prometheus AWS App Mesh, Amazon Athena,,,,, Amazon, Amazon DynamoDB AWS Batch AWS CloudFormation AWS CloudTrail AWS CodeArtifact CodeGuru, AWS Directory Service Amazon Elastic Compute Cloud (Amazon EC2), Amazon Evidently CloudWatch , Amazon Forecast,,,, (IAM), Amazon Managed Streaming para Apache Kafka (Amazon MSK AWS Organizations) AWS IoT Greengrass, AWS Ground Station Amazon Lightsail, AWS Identity and Access Management Amazon Logs,, CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor, Amazon Pinpoint, Amazon Virtual Private Cloud (Amazon VPC), Amazon Personalize, Amazon QuickSight, Amazon Simple Storage Service (AWS Migration Hub Refactor Spaces Amazon S3),	13 de junho de 2023

Amazon e. SageMaker AWS Transfer Family Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.

AWS Config Registrando exclusões por tipo de recurso	Com esta versão, AWS Config permite que você exclua tipos específicos de AWS recursos do rastreamento de inventário e do monitoram ento de conformidade e, ao mesmo tempo, rastreie todos os outros tipos de recursos compatíveis atualmente disponíveis AWS Config, incluindo aqueles que serão adicionados no futuro. Você pode usar esse recurso para se concentrar em recursos essenciais que estão sujeitos aos seus padrões de conformidade e governança. As atualizações da API para o gravador de configuração e o grupo de gravação são compatíveis com versões anteriores, o que significa que elas funcionam com versões anteriores da API PutConfig urationRecorder. Você pode continuar gerenciando quais tipos de recursos são registrad os exatamente da mesma forma que antes, sem usar as APIs novas ou atualizadas. Os seguintes tipos de dados foram adicionados: • RecordingStrategy • ExclusionByResourceTypes	9 de junho de 2023

Os seguintes tipos de dados foram atualizados:

- PutConfigurationGravador
- ConfigurationRecorder
- RecordingGroup

A seguinte página no guia do desenvolvedor foi atualizada:

- Seleção de quais recursos são registrados

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo Amazon Elastic Container Service (Amazon ECS), Amazon Keyspaces (para Apache Cassandra) (Amazon Keyspaces),,,,, Amazon AWS CodeArtifact 2.0 AWS Amplify AWS App Mesh AWS App Runner, Amazon Elastic Compute Cloud (AppStream Amazon EC2 AWS Signer), Amazon Evidently, Amazon Forecast, (AWS Identity and Access Management IAM), Amazon Pinpoint CloudWatch , Amazon, Amazon, Amazon Data Firehose. SageMaker AWS Transfer Family Para obter mais informações, consulte Tipos de recursos compatíveis.	5 de junho de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	10 de maio de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de recursos Amazon Route 53 Resolver, Amazon Elastic Compute Cloud (Amazon EC2) AWS IoT , Wireless, ,,, Amazon AWS Network Manager, Amazon Redshift AWS Device Farm, AWS Ground Station AppFlow Amazon Pinpoint,,, AWS AppConfig EC2 Image Builder AWS IoT, Amazon, Amazon Runtime AWS Panorama, CloudWatch SageMaker Amazon ECR e tipos de recursos. AWS Audit Manager Para obter mais informações, consulte Tipos de recursos compatíveis.	5 de maio de 2023
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar as alterações de configuração no`AWS::NetworkFirewall::TLSInspectionConfiguration` . Para obter mais informações, consulte Tipos de recursos compatíveis.	1º de maio de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Managed Workflows para AWS Amplify,, AWS App Mesh, Amazon AWS App Runner CloudFront AWS CodeArtifact, Amazon Elastic Compute Cloud, Amazon Kendra, Amazon Macie, Amazon Route 53, Amazon,, Amazon AWS Migration Hub Pinpoint AWS Transfer Family,, AWS Resilience Hub, Amazon, Directory Service e. SageMaker CloudWatch AWS AWS WAF Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	13 de abril de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	10 de abril de 2023
Aumento dos limites de serviço para pacotes de conformidade organizacional	Com esta versão, AWS Config oferece suporte a 350 AWS Config regras por conta em todos os pacotes de conformidade da organização. Para obter mais informações, consulte Limites de serviço.	3 de abril de 2023

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	3 de abril de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo Amazon AppStream 2.0, AWS Auto Scaling, Amazon Connect Amazon Elastic Compute Cloud, Amazon, HealthLak e Kinesis Video Stream EventBridge, Lookout AWS IoT TwinMaker for Vision, Network Manager, Amazon Pinpoint, Amazon Route 53 Application Recovery Controlle r e tipos de recursos. AWS RoboMaker Para obter mais informações, consulte Tipos de recursos compatíveis.	3 de abril de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Managed Workflows para Amazon AppFlow, Amazon AppStream 2.0 AWS App Runner, Amazon, Amazon, AWS CloudFormation,, CloudFront CloudWatch AWS CodeArtifact, Amazon Elastic Compute Cloud (Amazon EC2) AWS CodeCommit AWS Device Farm, Amazon Evidently, Amazon Forecast,, (IAM AWS IoT) CloudWatch ,, Amazon MemoryDB for Redis, AWS Ground Station Amazon AWS Identity and Access Management Pinpoint,,, Amazon Relational Database Service Database Service (AWS Panorama Amazon RDS) AWS Network Manager, Amazon Redshift e Amazon. SageMaker Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	30 de março de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS Audit Manager. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	3 de março de 2023
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de recursos AWS Elemental MediaPackage, Amazon EventBridge AWS IoT, (Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Lookout for Metrics, Amazon Lex AWS Budgets CodeGuru ,, AWS Device Farm Amazon Reviewer e outros tipos de recursos. Amazon Route 53 Resolver AWS RoboMaker Para obter mais informações, consulte Tipos de recursos compatíveis.	2 de março de 2023

Atualização de segurança do IAM	AWS Config agora rastreia as alterações na `AWSConfigMultiAccountSetupPolicy` política. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	27 de fevereiro de 2023
AWS Config Cobertura de recursos por região e disponibilidade	Com esta versão, AWS Config fornece informações de região para cada tipo de recurso suportado. Para obter informações sobre quais tipos de recursos são compatíveis em quais regiões, consulte Disponibilidade de recursos por região.	20 de fevereiro de 2023
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para gravar alterações de configuração no novo Amazon Interactive Video Service (Amazon IVS), Amazon Simple Storage Service (Amazon S3), Amazon Elastic Kubernetes Service AWS Glue(Amazon EKS) AWS IoT, Amazon Relational Database Service (Amazon RDS) e Managed Service for Apps Tipos de recursos do Cache Flink. Para obter mais informações, consulte Tipos de recursos compatíveis.	7 de fevereiro de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Managed Workflows para Apache Airflow, AWS IoT Amazon 2.0, Amazon CodeGuru Reviewer AppStream , Amazon Kinesis Video Streams AWS HealthLake, Amazon Route 53 Application Recovery Controller, Amazon Elastic Compute Cloud (Amazon EC2) AWS Device Farm, Amazon Pinpoint (IAM), Amazon e Amazon Logs. AWS Identity and Access Management GuardDuty CloudWatch Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	1° de fevereiro de 2023
Atualização de segurança do IAM	Como prática recomendada de segurança, a política do `ConfigConformsServiceRolePolicy` agora remove uma ampla permissão em nível de recurso para `config:DescribeConfigRules` . Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	12 de janeiro de 2023

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para o Amazon Managed Service for Prometheus AWS Audit Manager,,, () AWS Device Farm AWS Database Migration Service , Amazon Elastic Compute Cloud AWS DMS(Amazon EC2) AWS Directory Service,,, Amazon AWS Elemental MediaPackage Lightsail,,, Amazon,, Amazon, Amazon AWS Glue AWS IoT, Amazon Route 53 Application Recovery Controller AWS Network Manager, QuickSight Amazon AWS Resource Access Manager Simple Storage Service (Amazon S3) e Amazon Timen Amazon Timestream. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	10 de janeiro de 2023

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos EventBridge esquemas do Amazon MQ,,, AWS Cloud9 Amazon AWS AppConfig, Amazon Fraud Detector,,, Amazon AWS IoT Analytics Lightsail AWS IoT, AWS Elemental MediaPackage (MediaPackage), Amazon Route 53 Application Recovery Controller e tipos de recursos. AWS Resilience Hub AWS Transfer Family Para obter mais informações, consulte Tipos de recursos compatíveis.	5 de janeiro de 2023
AWS Config cobertura de recursos de regras	Com essa versão, AWS Config exibe a cobertura do tipo de recurso para um número maior de regras AWS Config gerenciadas.	21 de dezembro de 2022
AWS Config descoberta de regras	Com esta versão, AWS Config oferece suporte às páginas Lista de regras AWS Config gerenciadas por modo de avaliação, Lista de regras AWS Config gerenciadas por tipo de acionador e Lista de regras AWS Config gerenciadas por disponibilidade regional.	21 de dezembro de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for K-ISMS • Operational Best Practices for NIST 800 171 • Operational Best Practices for PCI DSS 3.2.1 • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for NZISM • Operational Best Practices for NIST 800-53 rev 5	19 de dezembro de 2022

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	9 de dezembro de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos Amazon CloudWatch RUM EventBridge, Amazon GuardDuty, Amazon, Amazon Simple Email Service (Amazon SES) AWS Backup AWS DataSync, ,, AWS Fault Injection Service e AWS FIS(). Para obter mais informações, consulte Tipos de recursos compatíveis.	9 de dezembro de 2022

AWS Config Conformidade proativa	Com esta versão, AWS Config oferece suporte à capacidade de verificar proativamente a conformidade com AWS Config as regras antes do provisionamento de recursos. Isso permite avaliar as definições de configuração de seus recursos antes de serem criados ou atualizados. Use AWS Config para rastrear as alterações de configuração feitas em seus recursos, seja no pré-provisionamento ou no pós-provisionamento, e verifique se os recursos correspondem às configurações desejadas. Os seguintes tipos de dados foram adicionados: • GetResourceEvaluationSummary • StartResourceAvaliação • ListResourceAvaliações Os seguintes tipos de dados foram atualizados: • DescribeConfigRulesFilters • GetComplianceDetailsByRecurso • EvaluationResultQualificador	28 de novembro de 2022

- EvaluationModeConfiguração

As seguintes páginas do guia do desenvolvedor foram atualizadas:

- Componentes de uma AWS Config regra
- Modo de avaliação e tipos de gatilho para AWS Config regras
- AWS Config Regras gerenciadas
- AWS Config Regras personalizadas
- Gerenciando suas AWS Config regras

Detecção de desvio como item de configuração (CI) para o gravador AWS Config de configuração	Com esta versão, AWS Config rastreia todas as alterações no gravador de configuração para indicar se o estado do gravador de configuração é diferente ou se desviou de seu estado anterior; por exemplo, se há atualizações nos tipos de recursos que você habilitou AWS Config para rastrear, se você interrompeu ou iniciou o gravador de configuração ou se excluiu ou desinstal ou o gravador de configura ção. O tipo de `AWS::Conf ig::ConfigurationR ecorder` recurso é um tipo de recurso do sistema AWS Config e o registro desse tipo de recurso é ativado por padrão em todas as regiões suportadas. A gravação para o tipo de recurso `AWS::Conf ig::ConfigurationR ecorder` vem sem custo adicional. Para obter mais informações, consulte Drift Detection for the Configuration Recorder.	18 de novembro de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos AWS IoT Events, AWS Cloud Map, EC2 Image Builder AWS DataSync,, AWS Glue, Amazon Route 53 Application Recovery Controller e Amazon Elastic Container Registry (Amazon ECR). Para obter mais informações, consulte Tipos de recursos compatíveis.	8 de novembro de 2022
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS CloudFormation. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	7 de novembro de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for Criminal Justice Information Services (CJIS) • Melhores práticas de segurança para a Amazon SageMaker • Security Best Practices for Amazon Elastic Container Registry Os seguintes pacotes de conformidade foram atualizados: • Operational Best Practices for MAS TRMG • Operational Best Practices for NCSC Cyber Assesment Framework • Operational Best Practices for NCSC Cloud Security Principles	27 de outubro de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS Certificate Manager Amazon Managed Workflows for Apache Airflow,, , AWS AppConfig Amazon Keyspaces AWS Amplify, Amazon, Amazon CloudWatch Connect, Amazon Elastic Compute Cloud (AWS Glue DataBrew Amazon EC2), Amazon Elastic Kubernetes Service (Amazon EKS), Amazon,, Amazon Fraud Detector, Amazon FSx FSx, Amazon, EventBridge AWS Fault Injection Service Amazon Location Service, Amazon Lex, Amazon Lightsail , GameLift Amazon Pinpoint, ,, AWS IoT, Amazon, Amazon Relational AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight Serviço de banco de dados (Amazon RDS), Amazon AWS RoboMaker Rekognition AWS Resource Groups,, Amazon Route 53, Amazon Simple Storage Service (Amazon S3) e. AWS Cloud Map AWS Security Token Service Para obter mais informações, consulte AWS	19 de outubro de 2022

	Políticas gerenciadas para o AWS Config.	
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de recursos do Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Email Service (Amazon SES AWS AppConfig) e do Amazon Elastic Compute Cloud (Amazon EC2). AWS Cloud Map AWS DataSync Para obter mais informações, consulte Tipos de recursos compatíveis.	6 de outubro de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de Amazon GuardDuty SageMaker AWS AppSync AWS Cloud Map, Amazon e AWS DataSync recursos. Para obter mais informações, consulte Tipos de recursos compatíveis.	04 de outubro de 2022
AWS Config suporta novo pacote de conformidade	Com esta versão, AWS Config atualiza o pacote de conformidade Operational Best Practices for SWIFT CSP.	04 de outubro de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for CMMC 2.0 Level 1 • Operational Best Practices for CMMC 2.0 Level 2 Os seguintes pacotes de conformidade foram atualizados: • Operational Best Practices for Amazon API Gateway • Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework • Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework • Operational Best Practices for CMMC Level 1 • Operational Best Practices for CMMC Level 2 • Operational Best Practices for CMMC Level 3 • Operational Best Practices for CMMC Level 4 • Operational Best Practices for CMMC Level 5 • Operational Best Practices for FFIEC	30 de setembro de 2022

	• Operational Best Practices for FedRAMP(Low) • Operational Best Practices for MAS Notice 655 • Operational Best Practices for NBC TRMG • Operational Best Practices for NIST 800 172	
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para AWS Glue. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	14 de setembro de 2022
AWS Config suporta novo pacote de conformidade	Com esta versão, AWS Config suporta o pacote de conformidade Operational Best Practices for SWIFT CSP.	9 de setembro de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon AppFlow, Amazon, Amazon CloudWatch RUM CloudWatch, Amazon CloudWatch Synthetics, Amazon Connect Customer Profiles, Amazon Connect Voice ID, Amazon DevOps Guru, Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Auto Scaling, Amazon EMR, Amazon, Amazon Schemas Amazon FinSpace, Amazon Fraud Detector, Amazon EventBridge, EventBridge Amazon GameLift Interactive Video Service (Amazon IVS), Amazon Managed Service para Apache Flink, EC2 Image Builder, Amazon Lex, Amazon Lightsail, Amazon Location Service, Amazon Lookout for Equipment, Amazon Lookout for Metrics, Amazon Lookout for Vision, Amazon Managed Blockchain, Amazon MQ, Amazon Nimble QuickSight Pinpoint, Amazon, StudioAmazon Amazon, controlador de recuperação de aplicativos Amazon Route 53, Amazon Simple	7 de setembro de 2022

Storage Service (Amazon Route 53 Resolver Amazon S3) Amazon SimpleDB, Amazon SimpleDB, Amazon Simple Email Service (Amazon SES), Amazon Timestrea m,,,,,,,,,,,, AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events, AWS IoT SiteWise AWS IoT TwinMaker, AWS Lake Formation, AWS License Manager, AWS Resilienc e Hub AWS Signer,, AWS Transfer Family e. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Melhores práticas operacionais para a Amazon CloudWatch • Operational Best Practices for Germany Cloud Computing Compliance Controls Catalog (C5) • Operational Best Practices for IRS 1075 Os seguintes pacotes de conformidade foram atualizados: • AWS Pacote de conformidade Control Tower Detective Guardrails • Operational Best Practices for CISA Cyber Essentials • Operational Best Practices for ENISA Cybersecurity guide for SMEs • Operational Best Practices for FDA Title 21 CFR Part 11 • Práticas recomendadas operacionais para o FedRAMP (Moderado) • Práticas recomendadas operacionais para a segurança da HIPAA	31 de agosto de 2022

	• Operational Best Practices for NIST Privacy Framework v1.0 • Operational Best Practices for NYDFS 23 • Operational Best Practices for RBI Cyber Security Framework for UCBs • Operational Best Practices for RBI MD-ITF	
Introdução AWS Config e atualizações do Custom Conformance Pack	Com esta versão, AWS Config atualiza as páginas Introduçã o AWS Config e Configuração AWS Config com o Console, introduzindo uma página de configuração com 1 clique e Configuração manual. AWS Config também atualiza a página Custom Conformance Pack com um passo a passo sobre como criar um arquivo YAML do pacote de conformid ade do zero.	25 de agosto de 2022

AWS Systems Manager Integração de documentos (documento SSM) com pacotes de conformidade	Com esta versão, é possível criar um modelo de pacote de conformidade com um documento SSM. Para obter mais informações sobre documentos SSM, consulte AWS Systems Manager Documentos no Guia do AWS Systems Manager usuário. Os seguintes tipos de dados foram atualizados: • PutConformancePacote • ConformancePackDetalhe • Modelos SSM DocumentDetails As seguintes páginas do guia do desenvolvedor foram atualizadas: • Implantando um pacote de conformidade usando o console AWS Config • Implantando um pacote de conformidade usando a interface de linha de comando AWS	24 de agosto de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para o Amazon Simple Email Service (Amazon SES) AWS DataSync, e. AWS Cloud Map Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	22 de agosto de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos Amazon Athena, Amazon Detective, Amazon SageMaker, Amazon Route 53 AWS Database Migration Service ,AWS DMS() AWS Glue, AWS Key Management Service ,AWS KMS() e Amazon Simple Email Service (Amazon SES). Para obter mais informações, consulte Tipos de recursos compatíveis.	16 de agosto de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for NIST 1800 25 • Operational Best Practices for NIST 800 181 • Operational Best Practices for ABS CCIG 2.0 Standard Workloads • Operational Best Practices for ABS CCIG 2.0 Material Workloads • Operational Best Practices for ACSC Essential 8 • Operational Best Practices for ACSC ISM • Operational Best Practices for APRA CPG 234 • Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1 • Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2 • Operational Best Practices for BNM RMiT • Operational Best Practices for NIST CSF	1º de agosto de 2022

Pontuação de conformidade para pacotes de conformidade	Com esta versão, AWS Config apresenta a pontuação de conformidade para pacotes de conformidade, que fornece uma visão de alto nível do estado de conformid ade de seus pacotes de conformidade. Você pode usá-lo para identificar, investigar e entender o nível de conformidade em seus pacotes de conformidade. Uma pontuação de conformid ade é a porcentagem do número de combinações de recursos e regras compatíve is em um pacote de conformid ade em comparação com o número total de combinações possíveis de regras e recursos no pacote de conformidade. Os seguintes tipos de dados foram atualizados: • ListConformancePac kCompliancePontuações • ConformancePackCom plianceScore As seguintes páginas do guia do desenvolvedor foram atualizadas: • Visualizando o AWS Config painel	26 de julho de 2022

	• Viewing Compliance Data in the Conformance Packs Dashboard • Gerenciar pacotes de conformidade (API)	
Atualização de segurança do IAM	A `ConfigConformsServiceRolePolicy` política agora concede permissão para publicar pontos de dados métricos na Amazon CloudWatch. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	25 de julho de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para o Amazon Elastic Container Service (Amazon ECS), Amazon, ElastiCache Amazon, EventBridge Amazon FSx, Amazon Managed Service para Apache Flink, Amazon Location Service, Amazon Managed Streaming para Apache Kafka, Amazon, Amazon Rekognition, QuickSight Amazon Amazon Simple Storage Service (AWS RoboMaker Amazon S3), Amazon Simple Email Service AWS Amplify(Amazon SES),,,,,,, (IAM Identity Center), EC2 Image Builder, AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center e Elastic Load Balancing. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	15 de julho de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos do Amazon Elastic Compute Cloud (Amazon EC2). Para obter mais informações, consulte Tipos de recursos compatíveis.	8 de julho de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de AWS Global Accelerator recursos. Para obter mais informações, consulte Tipos de recursos compatíveis.	5 de julho de 2022
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled • nlb-cross-zone-load-balancing-enabled	1° de julho de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for Canadian Centre for Cyber Security (CCCS) Medium Cloud Control Profile • Operational Best Practices for Gramm Leach Bliley Act (GLBA) • Operational Best Practices for GxP EU Annex 11 • Security Best Practices for Amazon Elastic Kubernetes Service (Amazon EKS) • Security Best Practices for Amazon Relational Database Service (Amazon RDS) • Melhores práticas de segurança para AWS Lambda Os seguintes pacotes de conformidade foram atualizados: • Operational Best Practices for AI and ML • Operational Best Practices for Amazon DynamoDB	30 de junho de 2022

	• Operational Best Practices for CIS Critical Security Controls v8 IG1 • Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Operational Best Practices for HIPAA Security • Operational Best Practices for NIST 800-53 rev 5 • Operational Best Practices for NIST CSF	
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de SageMaker recursos da Amazon. Para obter mais informações, consulte Tipos de recursos compatíveis.	29 de junho de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Route 53, WorkSpace s AWS Batch Amazon,, (IAM Access Analyzer AWS Database Migration Service) AWS Identity and Access Management Access Analyzer AWS DMS, () AWS Step Functions e Elastic Load Balancing. Para obter mais informações, consulte Tipos de recursos compatíveis.	14 de junho de 2022

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	13 de junho de 2022

AWS Config Integração com AWS Security Hub	Com esta versão, você pode ver os resultados das avaliações de regras AWS Config gerenciadas e personalizadas conforme descobertas em AWS Security Hub. O Security Hub transform a avaliações de regras em descobertas, que fornecem mais informações sobre os recursos afetados, como o nome do recurso da Amazon (ARN) e a data de criação. Essas descobertas podem ser visualizadas com outras descobertas do Security Hub, fornecendo uma visão geral abrangente de sua postura de segurança. Para obter mais informações, consulte Enviar avaliações de regras para o Security Hub	7 de junho de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para Amazon Athena, Amazon Detective, Amazon, GuardDuty Amazon Macie, Amazon Simple Email Service (Amazon SES AWS Glue),, () e. AWS Resource Access Manager AWS RAM AWS IAM Identity Center Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	31 de maio de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Security Best Practices for Amazon Elastic Container Service (Amazon ECS) • Security Best Practices for Amazon Elastic File System (Amazon EFS) • Melhores práticas de segurança para a Amazon CloudFront • Melhores práticas de segurança para AWS Auto Scaling • Melhores práticas de segurança para AWS Network Firewall • Melhores práticas de segurança para AWS Secrets Manager	31 de maio de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de AWS Step Functions recursos SageMaker e da Amazon. Para obter mais informações, consulte Tipos de recursos compatíveis.	26 de maio de 2022

AWS Config suporta novo pacote de conformidade	Com esta versão, AWS Config atualiza as melhores práticas operacionais para o pacote de conformidade NERC CIP BCSI.	20 de maio de 2022
Componentes de uma AWS Config regra	Com esta versão, AWS Config apresenta a página Componentes de uma AWS Config regra. A página discute a estrutura de definições de regras, metadados de regras e melhores práticas sobre como escrever regras com Python usando o Rules Developme nt Kit (RDK) e a AWS Config Rules Development Kit Library (AWS Config RDKLib).	9 de maio de 2022
Aumento dos limites de serviço para pacotes de conformidade organizacional	Com esta versão, AWS Config oferece suporte a 180 AWS Config regras por conta em todos os pacotes de conformid ade da organização. Para obter mais informações, consulte Limites de serviço.	6 de maio de 2022

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Melhores práticas de segurança para o Amazon OpenSearch Service • Security Best Practices for Amazon Redshift • Melhores práticas de segurança para AWS CloudTrail • Melhores práticas de segurança para AWS CodeBuild • Melhores práticas de segurança para AWS WAF	29 de abril de 2022
AWS Config atualiza a regra gerenciada	Com esta versão, AWS Config oferece suporte à regra gerenciada s3-resources-protected-by-backup-plan.	11 de abril de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões adicionais para obter informações sobre todo ou um armazenamento de dados de AWS CloudTrail eventos (EDS) específico, obter informações sobre todo ou um AWS CloudFormation recurso específico, obter uma lista de um grupo de parâmetros ou grupo de sub-rede do DynamoDB Accelerator (DAX), obter informações AWS Database Migration Service sobre AWS DMS() tarefas de replicação para sua conta na região atual que está sendo acessada e obter uma lista de todas as políticas de um tipo específico. AWS Organizations Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	7 de abril de 2022

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty	4 de abril de 2022

- vpc-peering-dns-resolution-check

AWS Config Regras de política personalizadas	Com esta versão, AWS Config permite que você crie regras de política AWS Config personalizadas usando o AWS CloudFormation Guard (guard). O Guard é uma policy-as-code linguagem que permite escrever políticas que são aplicadas AWS Config sem a necessidade de criar funções Lambda para gerenciar suas regras personalizadas. As regras escritas usando a política do Guard podem ser criadas no AWS Config console ou usando as APIs de AWS Config regras. As seguintes páginas do guia do desenvolvedor foram atualizadas: • Regras personalizadas do AWS Config • Criação AWS Config de regras personalizadas com o Guard Os seguintes tipos de dados foram atualizados: • Origem • CustomPolicyDetalhes • ConfigRuleEvaluationStatus • GetCustomRulePolicy	4 de abril de 2022

	• GetOrganizationCustomRulePolítica • OrganizationCustomPolicyRuleMetadados	
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo tipo de SecurityConfiguration recurso do Amazon EMR. Para obter mais informações, consulte Tipos de recursos compatíveis.	31 de março de 2022
AWS Config atualiza a regra gerenciada	Com esta versão, AWS Config oferece suporte à regra gerenciada de recursos de máquinas virtuais protegidos pelo plano de backup.	29 de março de 2022

AWS Config Integração com Amazon CloudWatch Metrics	Com esta versão, AWS Config agora oferece suporte ao rastreamento de suas métricas de AWS Config uso e sucesso com a Amazon CloudWatch na página AWS Config do painel. CloudWatch metrics é um serviço de monitoramento que fornece dados sobre o desempenho de seus sistemas, incluindo a capacidade de pesquisar, representar graficamente e criar alarmes sobre métricas sobre AWS recursos. No AWS Config painel, você pode ver qual tráfego está impulsionando seu AWS Config uso e as principais métricas de falhas que ocorreram em seu fluxo de trabalho. A seguinte página foi atualizada: • Visualizando o AWS Config painel	29 de março de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no novo tipo de recurso do Amazon GuardDuty Detector. Para obter mais informações, consulte Tipos de recursos compatíveis.	24 de março de 2022

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty	23 de março de 2022

	• waf-global-rule-not-empty	
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for CIS Critical Security Controls v8 IG1 • Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High • Operational Best Practices for MAS Notice 655 • Operational Best Practices for NIST 1800-25	16 de março de 2022

Atualização de segurança do IAM	As políticas `AWSConfigServiceRolePolicy` e `AWS_ConfigRole` agora concedem permissões adicionais para o AWS CloudFormation. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	14 de março de 2022
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config atualiza as seguintes regras gerenciadas: • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	10 de março de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos públicos do Amazon Elastic Container Registry. Para obter mais informações, consulte Tipos de recursos compatíveis.	4 de março de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos do Amazon Elastic Compute Cloud. Para obter mais informações, consulte Tipos de recursos compatíveis.	28 de fevereiro de 2022
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	25 de fevereiro de 2022

Registro e monitoramento na AWS Config atualização	Com esta versão, AWS Config atualiza a página Monitoramento AWS Config com EventBridge Eventos da Amazon para substituir as referências aos CloudWatch Eventos da Amazon. A Amazon EventBridge é a forma preferida de gerenciar seus eventos. CloudWatch Eventos e EventBridge são o mesmo serviço e API subjacentes, mas EventBridge oferecem mais recursos. As alterações feitas em um CloudWatch ou EventBridge aparecerão em cada console. Para obter mais informações, consulte Amazon. EventBridge	24 de fevereiro de 2022
AWS Página do SDK para AWS Config	Com esta versão, AWS Config introduz uma página Usando AWS Config com um AWS SDK. AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.	24 de fevereiro de 2022

Atualização da política de confiança do perfil do IAM de segurança	Com esta versão, AWS Config atualiza a declaraçã o de política de confiança do IAM para incluir proteções de segurança na política de confiança que restringem o acesso com `sourceARN` e/ou `sourceAccountId` para a operação AWS Security Token Service (AWS STS). Isso ajuda a garantir que o perfil do IAM acesse seus recursos somente em nome de usuários e cenários esperados. A seguinte página foi atualizad a: • Adicionar uma política de confiança do IAM à sua função	18 de fevereiro de 2022

Alterações na gravação global de tipos de recursos	AWS Config agora altera a forma como os novos tipos de recursos globais são registrados na AWS Config Gravação. Os tipos de recursos globais são AWS recursos que não exigem que você especifique uma região na criação. Antes dessa alteração, você poderia habilitar o registro de tipos de recursos globais em todas as regiões com suporte no AWS Config. Após essa alteração, os novos tipos de recursos globais integrados à AWS Config gravação só podem ser registrados na região de origem do serviço para a partição comercial e AWS GovCloud (Oeste dos EUA) para a partição. AWS GovCloud (US) Agora você poderá visualizar os itens de configuração desses novos tipos de recursos globais somente em sua região de origem e AWS GovCloud (Oeste dos EUA). Para obter uma lista das regiões de origem dos tipos de recursos globais integrados após fevereiro de 2022, consulte a tabela na página Registrar todos os tipos de recursos compatíveis.	18 de fevereiro de 2022

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissão para obter detalhes sobre os ambientes do Elastic Beanstalk e uma descrição das configurações do conjunto de configurações especificado do Elastic Beanstalk, obter um mapa das versões do Elasticsearch, descrever os grupos de opções disponíveis OpenSearch do Amazon RDS para um banco de dados e obter informações sobre uma configuração de implantação. CodeDeploy Agora, essa política também concede permissão para recuperar o contato alternativo especificado anexado a uma Conta da AWS, recuperar informações sobre uma AWS Organizations política, recuperar uma política de repositório do Amazon ECR, recuperar informações sobre uma regra arquivada AWS Config , recuperar uma lista de famílias de definição de tarefas do Amazon ECS, listar as unidades organizacionais (OUs) raiz ou principal da OU ou conta secundária especificada e listar as políticas anexadas à raiz,	10 de fevereiro de 2022

unidade organizacional ou conta de destino especificada. Para obter mais informaçõ es, consulte AWS Políticas gerenciadas para o AWS Config.

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-imutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version	10 de fevereiro de 2022

	• eks-cluster-supported-version • lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissão para criar grupos e fluxos de CloudWatch log da Amazon e para gravar registros nos fluxos de log criados. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	2 de fevereiro de 2022

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	31 de janeiro de 2022
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de AWS CodeDeploy recursos. Para obter mais informações, consulte Tipos de recursos compatíveis.	5 de janeiro de 2022

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de SageMaker recursos da Amazon. Para obter mais informações, consulte Tipos de recursos compatíveis.	20 de dezembro de 2021
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for ENISA Cybersecurity guide for SMEs	20 de dezembro de 2021
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for NIST 800 172 • Operational Best Practices for NIST 800 181 O seguinte pacote de conformidade foi atualizado: • Operational Best Practices for K-ISMS	18 de novembro de 2021

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for Amazon API Gateway • Melhores práticas operacionais para AWS Backup • Operational Best Practices for CISA Cyber Essentials • Melhores práticas operacionais para DevOps • Operational Best Practices for NIST Privacy Framework v1.0 Os seguintes pacotes de conformidade foram atualizados: • Operational Best Practices for FedRAMP(Low) • Operational Best Practices for FedRAMP(Moderate)	29 de outubro de 2021
AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em novos tipos de recursos do Amazon OpenSearch Service. Para obter mais informações, consulte Tipos de recursos compatíveis.	12 de outubro de 2021

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza o seguinte pacote de conformidade: • Operational Best Practices for MAS TRMG	12 de outubro de 2021

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for ABS CCIG 2.0 Material Workloads • Operational Best Practices for ABS CCIG 2.0 Standard Workloads • Operational Best Practices for ACSC Essential 8 • Operational Best Practices for ACSC ISM • Operational Best Practices for BNM RMiT • Operational Best Practices for CMMC Level 1 • Operational Best Practices for CMMC Level 2 • Operational Best Practices for CMMC Level 3 • Operational Best Practices for CMMC Level 4 • Operational Best Practices for CMMC Level 5 • Operational Best Practices for FDA Title 21 CFR Part 11 • Operational Best Practices for FFIEC • Operational Best Practices for MAS Notice 655	30 de setembro de 2021

	• Operational Best Practices for NBC TRMG • Operational Best Practices for NERC CIP • Operational Best Practices for NIST 800-53 rev 5	
Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissão para obter detalhes sobre um domínio/domínios do Amazon OpenSearch Service (OpenSearch Service) e obter uma lista detalhada de parâmetros para um determina do grupo de parâmetros de banco de dados do Amazon Relational Database Service (Amazon RDS). Essa política também concede permissão para obter detalhes sobre os ElastiCache snapshots da Amazon. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	8 de setembro de 2021

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos novos tipos de recursos do Amazon Elastic Compute Cloud. Para obter mais informações, consulte Tipos de recursos compatíveis.	7 de setembro de 2021

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config atualiza os seguintes pacotes de conformidade: • Operational Best Practices for APRA CPG 234 • Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 1 • Melhores práticas operacionais para o CIS AWS Foundations Benchmark v1.4 Level 2 • Operational Best Practices for NCSC Cloud Security Principles • Operational Best Practices for NCSC Cyber Assesment Framework • Operational Best Practices for NIST 800 171 • Operational Best Practices for NIST CSF • Operational Best Practices for RBI Cyber Security Framework for UCBs • Operational Best Practices for RBI MD-ITF • Operational Best Practices for NYDFS 23 • Operational Best Practices for PCI DSS 3.2.1	30 de agosto de 2021

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	20 de agosto de 2021
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte ao seguinte pacote de conformidade: • Operational Best Practices for NZISM	20 de agosto de 2021

Atualização da política do Amazon SNS para segurança	Com esta versão, AWS Config atualiza a declaração de política do IAM para o tópico do Amazon SNS ao usar funções vinculadas a serviços para incluir proteções de segurança que restringem o acesso com `sourceARN` e/ou `sourceAccountId` na política do tópico. Isso ajuda a garantir que o Amazon SNS acesse seus recursos somente em nome de usuários e cenários esperados. A seguinte página foi atualizada: • Permissões para o tópico Amazon SNS	17 de agosto de 2021

Atualização da AWS Lambda política de segurança	Com esta versão, AWS Config atualiza a política AWS Lambda baseada em recursos para regras AWS Config personalizadas para incluir proteções de segurança que restringem o acesso com `sourceARN` e/ou `sourceAccountId` na solicitação de invocação . Isso ajuda a garantir que você AWS Lambda esteja acessando seus recursos somente em nome dos usuários e cenários esperados . As seguintes páginas foram atualizadas: • AWS::Config::ConfigRule • Desenvolvendo uma regra personalizada para AWS Config	12 de agosto de 2021
AWS Config suporta novos tipos de recursos	Com essa versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de recursos do Amazon Kinesis. Para obter mais informações, consulte Tipos de recursos compatíveis.	6 de agosto de 2021

AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte ao seguinte pacote de conformidade: • Operational Best Practices for Esquema Nacional de Seguridad (ENS) High Os seguintes pacotes de conformidade foram atualizados: • Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework • Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Low • Operational Best Practices for Esquema Nacional de Seguridad (ENS) Medium • Operational Best Practices for HIPAA Security	30 de julho de 2021
AWS Lambda Funções de exemplo para regras AWS Config personalizadas	Com esta versão, AWS Config fornece funções de exemplo em Python em Example AWS Lambda Functions for AWS Config Rules (Python).	29 de julho de 2021

Atualização de segurança do IAM	As políticas `AWSConfigServiceRolePolicy` e `AWS_ConfigRole` agora concedem permissão para listar tags para um grupo de registros, listar tags para uma máquina de estado e listar todas as máquinas de estado. Essas políticas agora concedem permissão para obter detalhes sobre uma máquina de estado. Agora, essas políticas também oferecem suporte a permissões adicionais para Amazon EC2 Systems Manager (SSM), Amazon Elastic Container Registry, Amazon FSx, Amazon Data Firehose, Amazon Managed Streaming for Apache Kafka (Amazon MSK), Amazon Relational Database Service (Amazon RDS), Amazon Route 53, Amazon, Amazon Amazon Simple Notification Service,, e. SageMaker AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	28 de julho de 2021

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de AWS Backup recursos. Para obter mais informações, consulte Tipos de recursos compatíveis.	14 de julho de 2021
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte aos seguintes pacotes de conformidade: • Operational Best Practices for CIS Critical Security Controls v8 IG1 • Operational Best Practices for CIS Critical Security Controls v8 IG2 • Operational Best Practices for CIS Critical Security Controls v8 IG3 • Operational Best Practices for NIST 1800 25	09 de julho de 2021
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • ssm-document-not-public • s3-account-level-public-access-blocks-periodic	25 de junho de 2021

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	10 de junho de 2021

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissão para visualizar as permissões de AWS Systems Manager documentos e informações sobre o IAM Access Analyzer. Essas políticas agora oferecem suporte a tipos de AWS recursos adicionais para Amazon Kinesis, Amazon, ElastiCache Amazon EMR, Amazon Route 53 e AWS Network Firewall Amazon Relational Database Service (Amazon RDS). Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessárias para oferecer suporte a esses tipos de recursos. Agora, essas políticas também oferecem suporte à filtragem de funções do Lambda @Edge para a regra gerenciada AWS Config lambda-inside-vpc. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	8 de junho de 2021

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	19 de maio de 2021
AWS Config suporta novos tipos de recursos	Com essa versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de recursos do Amazon Elastic File System. Para obter mais informações, consulte Tipos de recursos compatíveis.	13 de maio de 2021

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissões que permitem fazer chamadas GET somente AWS Config para leitura para o API Gateway para oferecer suporte a uma regra de configuração para o API Gateway. Essas políticas também adicionam permissões que permitem AWS Config invocar as APIs somente para leitura do Amazon Simple Storage Service (Amazon S3), que são necessárias para suportar o novo tipo de recurso. `AWS::S3::AccessPoint` Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	10 de maio de 2021
AWS Config Regras personalizadas	As seguintes páginas do guia do desenvolvedor foram atualizadas: • Introdução às regras personalizadas para AWS Config • Desenvolvendo uma regra personalizada para AWS Config	30 de abril de 2021

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	15 de abril de 2021

Atualização de segurança do IAM	A `AWSConfigServiceRolePolicy` política e a `AWS_ConfigRole` política agora concedem permissão para visualizar informações sobre documentos AWS Systems Manager específicos. Agora AWS Backup, essas políticas também oferecem suporte a tipos de AWS recursos adicionais para Amazon Elastic File System ElastiCache, Amazon, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon SageMaker AWS Database Migration Service Kinesis, Amazon e Amazon Route 53. Essas alterações de permissão permitem AWS Config invocar as APIs somente para leitura necessárias para oferecer suporte a esses tipos de recursos. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Config.	14 de abril de 2021

Conformidade do pacote de conformidade como itens de configuração (CIs)	Com esta versão, AWS Config oferece suporte à conformidade do pacote de conformidade como itens de configuração. Isso permite que você: • Visualize um cronograma de alterações no estado de adequação dos seus pacotes de conformidade. • Agregue a adequação dos pacotes de conformidade em várias contas e regiões. • Use consultas avançadas para verificar a adequação dos seus pacotes de conformidade. Os seguintes tipos de dados foram atualizados: • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary As seguintes páginas do guia do desenvolvedor foram atualizadas: • Viewing Compliance Data in the Conformance Packs Dashboard	30 de março de 2021

	• Visualizar o cronograma do histórico de conformidade para pacotes de conformidade • Visualizando dados de conformidade no painel do Aggregator • Consultando o estado atual da configuração dos recursos AWS • Tipos de recursos compatíveis	
Atualização de paginação	Com essa versão, o recurso de consultas AWS Config avançadas agora oferece suporte à paginação para consultas que contêm funções agregadas, como COUNT e SUM. Agora você pode usar consultas avançadas para obter resultados completos para suas consultas agregadas por meio da paginação, que antes era limitada a 500 linhas. Para obter mais informações, consulte Consultando o estado atual da configuração dos recursos AWS	26 de março de 2021
Suporte de região	Com esta versão, AWS Config o AWS Config Rules agora é suportado na região Ásia-Pacífico (Osaka).	4 de março de 2021

AWS Config suporta novos tipos de recursos	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de recursos Amazon Elastic Container Registry, Amazon Elastic Container Service e Amazon Elastic Kubernete s Service. Para obter mais informações, consulte Tipos de recursos compatíveis.	25 de fevereiro de 2021
Suporte à criptografia do KMS	Com essa versão, você AWS Config pode usar a criptografia baseada em KMS em objetos entregues pelo AWS Config for S3 bucket delivery. Os seguintes tipos de dados foram atualizados: • DeliveryChannel • PutDeliveryCanal As seguintes páginas do guia do desenvolvedor foram atualizadas: • Permissões para a chave do KMS • Permissões para a função do IAM atribuída a AWS Config	16 de fevereiro de 2021

AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	16 de fevereiro de 2021
Suporte regional às consultas salvas	Com essa versão, agora há suporte para consultas salvas nas regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).	15 de fevereiro de 2021
Suporte regional à agregação de dados em várias contas e várias regiões	Com esta versão, a agregação de dados de várias contas e várias regiões agora é compatível na região UE (Estocolmo). Para obter mais informações, consulte Agregação de dados de várias regiões e várias contas.	15 de fevereiro de 2021
Suporte regional às consultas avançadas	Com esta versão, as consultas avançadas agora são suportadas nas regiões África (Cidade do Cabo) e Europa (Milão). Para obter mais informações, consulte Consultando o estado atual da configuração dos AWS recursos.	15 de fevereiro de 2021

AWS Config notificação de histórico de documentação disponível por meio de feed RSS	Agora você pode receber notificações sobre atualizações na AWS Config documentação assinando um feed RSS.	1º de janeiro de 2021

Atualizações anteriores

A tabela a seguir descreve o histórico de lançamento da documentação AWS Config antes de 31 de dezembro de 2020.

Alteração	Descrição	Data de lançamento
Suporte para consultas salvas	Com esta versão, AWS Config permite que você salve suas consultas. Depois de salvar a consulta, você pode pesquisá-la, copiá-la para o editor de consultas , editá-la ou excluí-la. Para obter mais informações sobre como salvar uma consulta, consulte Consultar usando o editor de consultas SQL (console) e Consulta usando o Editor de consultas SQL (AWS CLI). Para obter mais informações sobre APIs, consulte Referência da API do AWS Config : • PutStoredConsulta • GetStoredConsulta • ListStoredConsultas • DeleteStoredConsulta Também consulte Service Limits.	21 de dezembro de 2020

Alteração	Descrição	Data de lançamento
Suporte para verificações de processo	Com esta versão, AWS Config suporta verificações de processo, que é um tipo de AWS Config regra que permite rastrear suas tarefas externas e internas que exigem verificação como parte dos pacotes de conformidade. Com as verificaç ões de processo, você pode listar a conformidade dos requisitos e ações em um único local. Para obter mais informações sobre verificações de processo, consulte o AWS Config Verificaç ões de processo em um pacote de conformidade tópico e a API PutExternalde avaliação.	17 de dezembro de 2020

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	17 de dezembro de 2020
AWS Config apoios AWS Network Firewall	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos seus tipos de recursos AWS Network Firewall FirewallPolicy RuleGroup,, e do Firewall. Para ter mais informações, consulte Tipos de recursos compatíveis.	4 de dezembro de 2020

Alteração	Descrição	Data de lançamento
Atualização da documentação	AWS Config adicionou suporte para agregação de dados de recursos em toda a organização em uma conta de administrador delegado. Você pode usar uma conta de administr ador delegado para agregar dados de configuração e compatibilidade de recursos de todas as contas de membros de uma organização no AWS Organizations. Para obter mais informações, consulte PutConfigurationAggregator Configurar um agregador usando o console e. Registrar um administr ador delegado	4 de dezembro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Práticas recomendadas operacionais para a CMMC Nível 3 • Práticas recomendadas operacionais para a CMMC Nível 4 • Práticas recomendadas operacionais para a CMMC Nível 5 • Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Low • Práticas recomendadas operacionais para o Esquema Nacional de Seguridad (ENS) Medium • Práticas recomendadas operacionais para a Estrutura de Avaliação Cibernética do NCSC • Práticas recomendadas operacionais para a estrutura de segurança cibernética do RBI para UCBs	30 de outubro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Práticas recomendadas operacionais para o ACSC Essential 8 • Práticas recomendadas operacionais para o ISM do ACSC • Práticas recomendadas operacionais para IA e ML • Práticas recomendadas operacionais para o gerenciamento de ativos • Práticas recomendadas operacionais para BCP e DR • Práticas recomendadas operacionais para o EC2 • Práticas recomendadas operacionais para o K-ISMS • Práticas recomendadas operacionais para o balanceamento de carga • Práticas recomendadas operacionais para o Registro • Práticas recomendadas operacionais para o monitoramento • Práticas recomendadas operacionais para tecnologia sem servidor	22 de outubro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Práticas recomendadas operacionais do CPG 234 da APRA • Práticas recomendadas operacionais para o FedRAMP (Baixo) • Práticas recomendadas operacionais para o Aviso 655 do MAS • Práticas recomendadas de operação para as TRMG do NBC • Práticas recomendadas operacionais para o NCSC Cloud Security Principles • Práticas recomendadas operacionais para o RBI MD-ITF	15 de outubro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Práticas operacionais recomendadas para workloads de materiais do CCIG 2.0 da ABS • Práticas recomendadas operacionais para workloads padrão do CCIG da ABS 2.0 • Práticas recomendadas operacionais para o BNM RMit • Práticas recomendadas operacionais para a resiliência de dados • Práticas recomendadas operacionais para o data lakes e os serviços de análise • Práticas recomendadas operacionais para criptografia e gerenciamento de chaves • Operational Best Practices for FDA Title 21 CFR Part 11 • Práticas recomendadas operacionais para recursos acessíveis ao público • Práticas recomendadas operacionais para as TRMG da MAS • Práticas recomendadas operacionais para o NERC CIP BCSI • Práticas recomendadas operacionais para o NYDFS 23	8 de outubro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Melhores práticas operacionais para o pilar de confiabilidade do AWS Well-Architected Framework • Melhores práticas operacionais para o pilar de segurança do AWS Well-Architected Framework • Práticas recomendadas operacionais para a CMMC Nível 1 • Práticas recomendadas operacionais para a CMMC Nível 2 • Práticas recomendadas operacionais para serviços de computação • Práticas recomendadas operacionais para serviços de bancos de dados • Práticas recomendadas operacionais para serviços de gerenciamento e governança • Práticas recomendadas operacionais para serviços de rede e entrega de conteúdo • Práticas recomendadas operacionais para serviços de segurança, identidade e conformidade • Práticas recomendadas operacionais para serviços de armazenamento	26 de outubro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta novos pacotes de conformidade	• Operational Best Practices for FedRAMP(Moderate) • Operational Best Practices for FFIEC • Operational Best Practices for HIPAA Security • Práticas recomendadas operacionais para o NIST 800-53 rev 4 • Práticas recomendadas operacionais do NIST 800 171	28 de setembro de 2020
Atualização da documentação	Os tópicos do pacote de conformidade a seguir foram atualizados. • Pré-requisitos • Implantar um pacote de conformidade usando o console do AWS Config • Gerenciar pacotes de conformidade em todas as contas na organização	28 de setembro de 2020
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	17 de setembro de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta AWS WAF v2	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seu WebACL AWS WAF v2, IPset RegexPatt ernSet,,, e tipos de recursos. RuleGroup ManagedRuleSet Para ter mais informações, consulte Tipos de recursos compatíveis.	1.º de setembro de 2020
Atualização da documentação	Foi adicionada uma observação ao Acesso total ao AWS Config sobre a criação de permissões personali zadas que concedem acesso total. A documentação dos seguintes tipos de recurso foi atualizada: • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	24 de agosto de 2020
Atualização da documentação	Os modelos Práticas recomendadas operacionais para o PCI DSS 3.2.1 e Práticas recomendadas operacionais do NIST CSF foram atualizados.	14 de agosto de 2020
Atualização da documentação	Adição de exemplos de consultas de relação. Para ter mais informações, consulte Exemplos de consultas de relacionamento.	30 de julho de 2020

Alteração	Descrição	Data de lançamento
Atualização da documentação	Os seguintes tipos de dados foram atualizados: • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatus • GetOrganizationConformancePackDetailedStatus	23 de julho de 2020
AWS Config suporta o tipo de recurso AWS Systems Manager	Com essa versão, você pode usar AWS Config para registrar alterações de configuração no tipo de recurso de dados de arquivo do AWS Systems Manager. Para ter mais informações, consulte Tipos de recursos compatíveis.	9 de julho de 2020
Atualização da documentação	Os modelos Melhores práticas operacionais para gerenciamento de AWS identidade e acesso e Práticas recomendadas operacionais para o PCI DSS 3.2.1 foram atualizados.	9 de julho de 2020

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check	9 de julho de 2020

Alteração	Descrição	Data de lançamento
	• rds-cluster-deletion-protection-enabled • rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	
Suporte regional à agregação de dados em várias contas e várias regiões	Com esta versão, a agregação de dados multiconta e multirregional agora é suportada nas regiões Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein). Para obter mais informações, consulte Multi-Account Multi-Region Data Aggregation e Solução de problemas para agregação de dados multirregionais de várias contas.	1º de julho de 2020

Alteração	Descrição	Data de lançamento
Suporte regional às consultas avançadas	Com esta versão, as consultas avançadas agora são suportadas nas regiões Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein). Para ter mais informações, consulte Consultar o estado atual da configuração dos recursos da AWS.	1º de julho de 2020
Atualização da documentação	A documentação dos seguintes tipos de recurso foi atualizada: • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	30 de junho de 2020
Atualização da documentação	A documentação foi atualizada com informações sobre segurança do AWS Config. Consulte Segurança em AWS Config.	24 de junho de 2020
Atualização da documentação	AWS Control Tower O modelo do Detective Guardrails Conformance Pack foi atualizado. Para ter mais informações, consulte AWSPacote de conformidade Control Tower Detective Guardrails.	4 de junho de 2020

Alteração	Descrição	Data de lançamento
AWS Config suporta um novo pacote de conformidade	Com esta versão, AWS Config oferece suporte às melhores práticas operacionais para o pacote de conformidade CSF do NIST. Para ter mais informações, consulte Práticas recomendadas operacionais do NIST CSF .	29 de maio de 2020
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	28 de maio de 2020

Alteração	Descrição	Data de lançamento
Suporte de administrador delegado	Com esta versão, você pode implantar AWS Config regras e pacotes de conformidade de qualquer conta de membro delegada em sua organização, além da conta de gerenciamento. Para obter mais informações sobre APIs, consulte Referência da API do AWS Config : • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatus • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatus • GetOrganizationConformancePackDetailedStatus Para ter mais informações, consulte Service Limits.	27 de maio de 2020

Alteração	Descrição	Data de lançamento
AWS Config regras Suporte regional	Com esta versão, poucas AWS Config regras são suportadas nas regiões da África (Cidade do Cabo) e Europa (Milão). Para obter uma lista detalhada de regras e as regiões nas quais elas têm suporte, consulte Lista de regras AWS Config gerenciadas.	28 de abril de 2020
AWS Config suporta novos pacotes de conformidade	Com esta versão, AWS Config oferece suporte a dois pacotes de conformidade. • AWS Pacote de conformidade Control Tower Detective Guardrails • Melhores práticas operacionais para o CIS Para ter mais informações, consulte Exemplos de modelos de pacote de conformidade.	22 de abril de 2020
AWS Config suporta AWS Secrets Manager	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seu segredo do Secrets Manager. Para ter mais informações, consulte Tipos de recursos compatíveis.	20 de abril de 2020

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	16 de abril de 2020
Suporte regional aos pacotes de conformidade	Com esta versão, os pacotes de conformidade agora são suportados na Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein). Para ter mais informações, consulte Conformance Packs.	8 de abril de 2020
Atualização da documentação	AWS Config os limites estão disponíveis neste guia do desenvolvedor. Para ter mais informações, consulte Service Limits.	8 de abril de 2020
Atualização da documentação	Recursos de terceiros que são gerenciados (ou seja, criados/atualizados/excluídos) por meio AWS CloudFormation do registro são automaticamente rastreados como itens de configuração. AWS Config Para ter mais informações, consulte Configurações de registro para recursos de terceiros.	30 de março de 2020

Alteração	Descrição	Data de lançamento
Atualização da documentação	As regras AWS Config gerenciadas são atualizadas para incluir Região da AWS informações. Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	27 de março de 2020
AWS Config suporta o tipo de recurso Amazon SNS	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seu tópico do Amazon SNS. Para ter mais informações, consulte Tipos de recursos compatíveis.	6 de março de 2020
Suporte regional à agregação de dados em várias contas e várias regiões	Com esta versão, a agregação de dados de várias contas e várias regiões agora é compatível na região UE (Estocolmo). Para ter mais informações, consulte Multi-Account Multi-Region Data Aggregation.	5 de março de 2020
Suporte regional às consultas avançadas	Com esta versão, as consultas avançadas agora são compatíveis na região UE (Estocolmo). Para ter mais informações, consulte Consultar o estado atual da configuração dos recursos da AWS.	5 de março de 2020

Alteração	Descrição	Data de lançamento
AWS Config permite que você execute consultas avançadas com agregadores de configuração	Com esta versão, AWS Config adiciona suporte para executar consultas avançadas com base nas propriedades de configuração de recursos com agregadores de configuração, permitindo que você execute as mesmas consultas em várias contas e regiões. Para ter mais informações, consulte Consultar o estado atual da configuração dos recursos da AWS. Com esta versão, AWS Config adiciona `SelectAggregateResourceConfig` API. Para obter mais informações, consulte SelectAggregateResourceConfigna Referência AWS Config da API:	28 de fevereiro de 2020
AWS Config suporta o tipo de recurso Amazon SQS	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em sua fila do Amazon SQS. Para ter mais informações, consulte Tipos de recursos compatíveis.	13 de fevereiro de 2020

Alteração	Descrição	Data de lançamento
AWS CloudFormation suporte para pacotes de conformidade	Com esta versão, foi adicionado AWS CloudFormation suporte para os seguintes recursos: `AWS::Config::ConformancePack` `OrganizationConformancePack` e. • AWS::Config::ConformancePack Use o `AWS::Config::ConformancePack` recurso para criar um Pacote de Conformidade que é uma coleção de AWS Config regras que podem ser facilmente implantadas em uma conta, em uma região e em toda a organização. AWS • AWS::Config::OrganizationConformancePacote Use o `AWS::Config::OrganizationConformancePack` recurso para criar um Pacote de Conformidade Organizacional que tenha informações sobre pacotes de conformidade AWS Config criados nas contas dos membros.	13 de fevereiro de 2020

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	20 de dezembro de 2019

Alteração	Descrição	Data de lançamento
Configurações de gravação para tipos de recursos personalizados	Com esta versão, AWS Config introduz o suporte para registrar configurações para tipos de recursos personalizados. Você pode publicar os dados de configuração de recursos de terceiros, visualizar AWS Config e monitorar o inventário de recursos e o histórico de configura ção usando o AWS Config console e as APIs. Para ter mais informações, consulte Configurações de registro para recursos de terceiros. Para obter mais informações sobre APIs, consulte Referência da API do AWS Config : • DeleteResourceConfig • PutResourceConfig	20 de novembro de 2019

Alteração	Descrição	Data de lançamento
Pacotes de conformidade	Com esta versão, AWS Config apresenta pacotes de conformid ade. Os pacotes de conformidade permitem que você empacote uma coleção de AWS Config regras e ações de remediação que podem ser implantadas juntas como uma única entidade em toda a organizaç ão. AWS Para ter mais informações, consulte Conformance Packs. Para obter mais informações sobre APIs, consulte Referência da API do AWS Config : • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformancePacotes • DescribeConformancePacotes • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatus • GetConformancePackComplianceDetalhes • GetConformancePackComplianceResumo • GetOrganizationConformancePackDetailedStatus, • PutConformancePacote	19 de novembro de 2019

Alteração	Descrição	Data de lançamento
	• PutOrganizationConformancePack	
AWS Config suporta os tipos OpenSearch de serviços e AWS Key Management Service recursos da Amazon	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em seu domínio e AWS Key Management Service chave do Amazon OpenSearch Service. Para ter mais informações, consulte Tipos de recursos compatíveis.	11 de novembro de 2019
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-deletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	10 de outubro de 2019

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo de recurso Amazon RDS	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seu banco de dados e banco de dados do Amazon Relational Database Service (Amazon RDS). ClusterSnapshot Para ter mais informações, consulte Tipos de recursos compatíveis.	17 de setembro de 2019
AWS Config suporta o tipo de recurso Amazon QLDB	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração no tipo de recurso de contabilidade Amazon Quantum Ledger Database (QLDB) do Amazon Quantum Ledger Database (QLDB). Para ter mais informações, consulte Tipos de recursos compatíveis.	10 de setembro de 2019

Alteração	Descrição	Data de lançamento
AWS Config permite que você aplique a correção automática em recursos não compatíveis, conforme avaliado pelas Regras AWS Config	Com esta versão, AWS Config introduz o suporte para aplicar a correção automática usando documentos de AWS Systems Manager automação em recursos não compatíveis, conforme avaliado pelas Regras. AWS Config Para ter mais informações, consulte Correção de recursos não compatíveis com regras AWS Config. Com esta versão, AWS Config adiciona as seguintes novas APIs. Para obter mais informações, consulte a Referência da API do AWS Config : • PutRemediationExceções • DescribeRemediationExceções • DeleteRemediationExceções	5 de setembro de 2019

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config oferece suporte às seguintes regras gerenciadas: • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	22 de agosto de 2019

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config atualiza as seguintes regras gerenciadas: • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	31 de julho de 2019
AWS Config suporta tipos de recursos do Amazon EC2	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos seguintes recursos do Amazon EC2: VPCendpoint, VPC e VPCEndpoi ntService. PeeringConnection Para ter mais informações, consulte Tipos de recursos compatíveis.	12 de julho de 2019

Alteração	Descrição	Data de lançamento
AWS Config permite que você gerencie AWS Config regras Contas da AWS em toda a organização	Com esta versão, AWS Config introduz o suporte para gerenciar AWS Config regras em toda Contas da AWS a organização. Você pode criar, atualizar e excluir AWS Config regras de forma centralizada em todas as contas da sua organização. Para ter mais informações, consulte Gerenciando AWS Config regras em todas as contas da sua organização. Para obter mais informações sobre APIs, consulte Referência da API do AWS Config : • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatus • DeleteOrganizationConfigRule	9 de julho de 2019
AWS Config suporta os tipos de recursos Amazon S3 e Amazon EC2	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no AccountPublicAccessBlock recurso Amazon S3 e nos seguintes recursos do Amazon EC2 NatGateway; EgressOnlyInternetGateway,, e. FlowLog Para ter mais informações, consulte Tipos de recursos compatíveis.	17 de maio de 2019

Alteração	Descrição	Data de lançamento
AWS Config atualiza as regras gerenciadas	Com esta versão, AWS Config atualiza as seguintes regras gerenciadas: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	7 de maio de 2019
AWS Config permite que você exclua uma ação de remediação usando AWS Management Console.	Com esta versão, AWS Config introduz o suporte para excluir uma ação de remediação usando. AWS Management Console Para ter mais informações, consulte Correção de recursos não compatíveis com regras AWS Config.	24 de abril de 2019
AWS Config suporta novas regras gerenciadas	Esta versão oferece suporte a uma nova regra gerenciada: fms-shield-resource-policy-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	7 de abril de 2019

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo de recurso Amazon API Gateway	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração nos seguintes recursos do Amazon API Gateway: Api (WebSocket API), RestApi (API REST), Stage (estágio WebSocket da API) e Stage (estágio da API REST). Para ter mais informações, consulte Tipos de recursos compatíveis.	20 de março de 2019
AWS Config permite que você execute consultas avançadas	Com esta versão, AWS Config adiciona suporte para executar consultas avançadas com base nas propriedades de configuração de recursos. Para ter mais informações, consulte Consultar o estado atual da configuração dos recursos da AWS. Com esta versão, AWS Config adiciona `SelectResourceConf ig` API. Para obter mais informaçõ es, consulte SelectResourceConfig na Referência da AWS Config API:	19 de março de 2019

Alteração	Descrição	Data de lançamento
AWS Config permite que você atribua tags aos seus AWS Config recursos	Com esta versão, AWS Config introduz o suporte ao controle de acesso baseado em tags para três AWS Config recursos — `ConfigRule`, `ConfigurationAggregator`, e `AggregationAuthorization` Para ter mais informações, consulte Marcar os recursos do AWS Config. Com esta versão, você pode adicionar, remover ou listar tags de seus recursos do AWS Config usando as APIs a seguir. Para obter mais informações, consulte a Referência da API do AWS Config : • ListTagsForResource • TagResource • UntagResource	14 de março de 2019

Alteração	Descrição	Data de lançamento
AWS Config permite que você aplique remediação em recursos não compatíve is, conforme avaliado pelas Regras AWS Config	Com esta versão, AWS Config introduz o suporte para aplicar remediação usando documentos de AWS Systems Manager automação em recursos não compatíveis, conforme avaliado pelas Regras. AWS Config Para ter mais informaçõ es, consulte Correção de recursos não compatíveis com regras AWS Config. Com esta versão, AWS Config adiciona as seguintes novas APIs. Para obter mais informações, consulte a Referência da API do AWS Config : • DeleteRemediationConfiguração • DescribeRemediationConfigur ações • DescribeRemediationExecutio nStatus • PutRemediationConfigurações • StartRemediationExecução	12 de março de 2019

Alteração	Descrição	Data de lançamento
AWS Config suporta AWS Config regras na região da China (Ningxia)	Esta versão suporta apenas 54 AWS Config regras na região da China (Ningxia). Para ter mais informações, consulte Lista de regras AWS Config gerenciadas. No entanto, atualmente AWS Config não oferece suporte às seguintes regras na região da China (Ningxia): • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check	12 de março de 2019

Alteração	Descrição	Data de lançamento
	• fms-webacl-rulegroup-association-check • guardduty-enabled-centralized • lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config suporta novas regras gerenciad as	Esta versão é compatível com as seguintes novas regras gerenciadas: • iam-user-mfa-enabled • s3-bucket-policy-grantee-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	21 de janeiro de 2019

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo de recurso Service Catalog	Com essa versão, você pode usar AWS Config para registrar alteraçõe s de configuração nos seguintes recursos do Service Catalog: CloudFromation produto, produto provisionado e portfólio. Para ter mais informações, consulte Tipos de recursos compatíveis.	11 de janeiro de 2019
Suporte a regras vinculadas a serviços AWS Config	Com esta versão, AWS Config adiciona uma nova regra de configuração gerenciada que oferece suporte a outros AWS serviços para criar AWS Config regras em sua conta. Para ter mais informaçõ es, consulte Regras vinculadas ao serviço AWS Config.	20 de novembro de 2018

Alteração	Descrição	Data de lançamento
AWS Config permite agregar dados de configuração de recursos AWS	Com esta versão, AWS Config introduz o suporte para agregar os dados de configuração dos AWS recursos. Para ter mais informações, consulte Como visualizar dados de conformidade e inventário no painel do agregador. Com esta versão, AWS Config adiciona as seguintes novas APIs. Para obter mais informações, consulte a Referência da API do AWS Config : • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceConta • GetAggregateResourceConfig • ListAggregateDiscoveredResources	19 de novembro de 2018
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	19 de novembro de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	12 de novembro de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	24 de outubro de 2018
Suporte ao histórico de compatibilidade	Com esta versão, AWS Config agora oferece suporte ao armazenamento do histórico de conformidade dos recursos, conforme avaliado pelas AWS Config Regras. Para ter mais informações, consulte Visualizar o cronograma do histórico de conformidade para recursos.	18 de outubro de 2018
Suporte regional à agregação de dados em várias contas e várias regiões	Como esta versão, a agregação de dados de várias contas e várias regiões agora é compatível em seis novas regiões. Para ter mais informações, consulte Multi-Account Multi-Region Data Aggregation.	4 de outubro de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta permissões em nível de recurso para ações de APIs de regras AWS Config	Com esta versão, AWS Config oferece suporte a permissões em nível de recurso para determina das ações da API de AWS Config regras. Para obter mais informações sobre as APIs compatíveis, consulte Permissões em nível de recurso suportadas para AWS Config ações da API Rule.	1º de outubro de 2018
AWS Config suporta o tipo CodePipeline de recurso	Com essa versão, você pode usar AWS Config para registrar alteraçõe s de configuração no tipo de AWS CodePipeline recurso. Para ter mais informações, consulte Tipos de recursos compatíveis.	12 de setembro de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	5 de setembro de 2018
AWS Config suporta o tipo de recurso AWS Systems Manager	Com essa versão, você pode usar AWS Config para registrar alterações de configuração nos tipos de recursos de conformidade de patches e de associação do AWS Systems Manager. Para ter mais informações, consulte Tipos de recursos compatíveis.	9 de agosto de 2018

Alteração	Descrição	Data de lançamento
AWS Config permite que você exclua seus AWS Config dados usando AWS Management Console	Com esta versão, AWS Config introduz o suporte para o uso AWS Management Console do período de retenção. No AWS Managemen t Console, você pode selecionar um período de retenção de dados personalizado para seu`ConfigurationItems`. Para ter mais informações, consulte Excluindo dados AWS Config.	7 de agosto de 2018
AWS Config suporta o tipo AWS Shield de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no tipo de recurso de AWS Shield proteção. Para ter mais informações, consulte Tipos de recursos compatíveis.	7 de agosto de 2018
AWS Config apoios AWS PrivateLink	Com esta versão, AWS Config oferece suporte AWS PrivateLink, permitindo que você roteie dados entre sua Amazon Virtual Private Cloud (VPC) e AWS Config totalmente dentro da rede. AWS Para ter mais informações, consulte Usando AWS Config com a interface Amazon VPC Endpoints.	31 de julho de 2018

Alteração	Descrição	Data de lançamento
AWS Config permite que você exclua seus AWS Config dados	Com esta versão, AWS Config introduz suporte para o período de retenção. AWS Config permite que você exclua seus dados especific ando um período de retenção para seus`ConfigurationItems` . Para ter mais informações, consulte Excluindo dados AWS Config. Com esta versão, AWS Config adiciona as seguintes novas APIs. Para obter mais informações, consulte a Referência da API do AWS Config : • PutRetentionConfiguração • DescribeRetentionConfigurações • DeleteRetentionConfiguração	25 de maio de 2018
AWS Config suporta novas regras gerenciad as	Esta versão oferece suporte às estas duas novas regras gerenciadas: • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	10 de maio de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo AWS X-Ray de recurso	Com essa versão, você pode usar AWS Config para registrar alterações de configuração no tipo de AWS X-Ray EncryptionConfig recurso. Para ter mais informações, consulte Tipos de recursos compatíveis.	1º de maio de 2018
AWS Config suporta o tipo de AWS Lambda recurso e uma nova regra gerenciada	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no tipo de recurso da AWS Lambda função. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão também é compatível com a regra gerenciada lambda-function-public-access-prohibited. Para ter mais informações, consulte AWS Config Regras gerenciadas.	25 de abril de 2018
AWS Config suporta o tipo AWS Elastic Beanstalk de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos recursos do AWS Elastic Beanstalk aplicativo, da versão do aplicativo e do ambiente. Para ter mais informações, consulte Tipos de recursos compatíveis.	24 de abril de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão oferece suporte às estas duas novas regras gerenciadas: • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	4 de abril de 2018

Alteração	Descrição	Data de lançamento
Agregação de dados de várias regiões e várias contas	Com esta versão, AWS Config introduz a agregação de dados multiconta e multirregional. Esse recurso permite agregar AWS Config dados de várias contas ou de uma organização e várias regiões em uma conta agregadora. Para ter mais informações, consulte Multi-Account Multi-Region Data Aggregation. Com esta versão, AWS Config adiciona as seguintes novas APIs. Para obter mais informações, consulte a Referência da API do AWS Config : • PutConfigurationAgregador • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAutorização • DescribeAggregationAutorizações • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRegra • DescribeConfigurationAgregadores • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAutorização • DeleteConfigurationAgregador	4 de abril de 2018

Alteração	Descrição	Data de lançamento
Monitoramento AWS Config com Amazon CloudWatch Events	Com esta versão, use o Amazon CloudWatch Events para detectar e reagir às mudanças no status dos AWS Config eventos. Para ter mais informações, consulte Monitoramento AWS Config com a Amazon EventBridge.	29 de março de 2018
Nova operação da API	Com esta versão, AWS Config adiciona suporte à BatchGetResourceConfigAPI, permitindo que você recupere em lote o estado atual de um ou mais dos seus recursos.	20 de março de 2018
AWS Config suporta o tipo AWS WAF RuleGroup de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração no AWS WAF RuleGroup e nos recursos RuleGroup regionais do AWS WAF. Para ter mais informações, consulte Tipos de recursos compatíveis.	15 de fevereiro de 2018

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	25 de janeiro de 2018
AWS Config suporta o tipo de recurso do Elastic Load Balancing	Com essa versão, você pode usar AWS Config para registrar alterações de configuração em seus balanceadores de carga clássicos do Elastic Load Balancing. Para ter mais informações, consulte Tipos de recursos compatíveis.	17 de novembro de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta a Amazon CloudFront e o tipo AWS WAF de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em sua CloudFront distribuição e distribuição de streaming. Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos seguintes recursos AWS WAF e nos recursos AWS WAF regionais: regra baseada em taxa, regra e Web ACL. Para ter mais informações, consulte Tipos de recursos compatíveis.	15 de novembro de 2017
AWS Config suporta o tipo AWS CodeBuild de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em seus AWS CodeBuild projetos. Para ter mais informações, consulte Tipos de recursos compatíveis.	20 de outubro de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta recursos de Auto Scaling e uma nova regra gerenciada	Com esta versão, você pode usar AWS Config para registrar alterações de configuração nos seguintes recursos do Auto Scaling: grupos, configuração de lançamento, ação agendada e política de escalabilidade. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão também é compatível com a seguinte regra gerenciada: • autoscaling-group-elb-healthcheck-required Para ter mais informações, consulte AWS Config Regras gerenciadas.	18 de setembro de 2017
AWS Config suporta o tipo AWS CodeBuild de recurso	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em seus AWS CodeBuild projetos. Para ter mais informações, consulte Tipos de recursos compatíveis.	20 de outubro de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta recursos de Auto Scaling e uma nova regra gerenciada	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração nos seguintes recursos do Auto Scaling: grupos, configuração de lançamento, ação agendada e política de escalabil idade. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão também é compatível com a seguinte regra gerenciada: • autoscaling-group-elb-healthcheck-required Para ter mais informações, consulte AWS Config Regras gerenciadas.	18 de setembro de 2017
AWS Config suporta o tipo de recurso de tabela do DynamoDB e uma nova regra gerenciada	Com essa versão, você pode usar AWS Config para registrar alterações de configuração em suas tabelas do DynamoDB. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão é compatível com a seguinte regra gerenciada: • dynamodb-autoscaling-enabled Para ter mais informações, consulte AWS Config Regras gerenciadas.	8 de setembro de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta duas novas regras gerenciadas para o Amazon S3	Esta versão oferece suporte a duas novas regras gerenciadas: • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited Para ter mais informações, consulte AWS Config Regras gerenciadas.	14 de agosto de 2017
Nova página no AWS Config console	Você pode usar o Painel no AWS Config console para ver o seguinte: • Número total de recursos • Número total de regras • Número de recursos não compatíveis • Número de regras não compatíveis Para ter mais informações, consulte Visualizando o AWS Config painel.	17 de julho de 2017
Nova operação da API	Você pode usar a GetDiscoveredResourceCountsoperação para retornar o número de tipos de recursos, o número de cada tipo de recurso e o número total de recursos que estão AWS Config sendo registrados em uma região para você Conta da AWS.	17 de julho de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo de recurso de AWS CloudFormation pilha e uma nova regra gerenciada	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em suas AWS CloudFormation pilhas. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão é compatível com a seguinte regra gerenciada: • cloudformation-stack-notification-check Para ter mais informações, consulte AWS Config Regras gerenciadas.	6 de julho de 2017
Conteúdo novo e atualizado	Esta versão adiciona suporte AWS Config às regras na região do Canadá (Central) e na região da América do Sul (São Paulo). Para todas as regiões que oferecem suporte ao AWS Config Config Rules, consulte Regiões da AWS e Endpoints no. Referência geral da AWS	5 de julho de 2017

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	AWS Config As regras estão disponíveis na AWS GovCloud (US) região. Para obter mais informações, consulte o AWS GovCloud (US) Guia de usuário do . Para regiões que oferecem suporte AWS Config, consulte Regiões da AWS e Endpoints no Referência geral da AWS.	8 de junho de 2017
AWS Config suporta o tipo de recurso de CloudWatch alarme da Amazon e três novas regras gerenciadas	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em seus CloudWatch alarmes da Amazon. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão oferece suporte a três novas regras gerenciadas: • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check Para ter mais informações, consulte AWS Config Regras gerenciadas.	1 de junho de 2017

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão oferece suporte para especificar o número de versão do aplicativo para as seguintes regras gerenciadas: • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required Para ter mais informações, consulte AWS Config Regras gerenciadas.	1 de junho de 2017
Conteúdo novo e atualizado	Esta versão adiciona suporte AWS Config às regras na região Ásia-Pacífico (Mumbai). Para obter mais informações, consulte Regiões da AWS e endpoints no Referência geral da AWS.	27 de abril de 2017

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão oferece suporte a uma experiência de console atualizado para adicionar regras gerenciadas do AWS Config à sua conta, pela primeira vez. Ao configurar AWS Config regras pela primeira vez ou em uma nova região, você pode pesquisar regras AWS gerenciadas por nome, descrição ou rótulo. Você pode escolher Select all (Selecionar tudo) para selecionar todas as regras ou escolher Clear all (Limpar tudo) para limpar todas as regras. Para obter mais informações, consulte Adicionar, visualizar, atualizar e excluir regras (console).	5 de abril de 2017

Alteração	Descrição	Data de lançamento
AWS Config suporta novas regras gerenciadas	Esta versão é compatível com as seguintes novas regras gerenciadas: • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	21 de fevereiro de 2017
Conteúdo novo e atualizado	Esta versão adiciona suporte às AWS Config regras na região da Europa (Londres). Para obter mais informações, consulte Regiões da AWS e endpoints no no Referência geral da AWS.	21 de fevereiro de 2017
Conteúdo novo e atualizado	Esta versão adiciona AWS CloudFormation modelos para regras AWS Config gerenciadas. Você pode usar os modelos para criar regras gerenciadas para a sua conta. Para ter mais informações, consulte Criar regras gerenciadas do AWS Config com modelos do AWS CloudFormation.	16 de fevereiro de 2017

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão inclui o suporte para um novo modo de teste para a API `PutEvaluations` . Defina o parâmetro `TestMode` como verdadeiro em sua regra personali zada para verificar se a função AWS Lambda entregará os resultados de avaliação para o AWS Config. Não houve atualizações nas suas avaliações existentes e os resultado s da avaliação não foram enviados para o AWS Config. Para obter mais informações, consulte PutEvaluationsa Referência AWS Config da API.	16 de fevereiro de 2017
Conteúdo novo e atualizado	Esta versão adiciona suporte para AWS Config regras nas regiões Ásia-Pacífico (Seul) e Oeste dos EUA (Norte da Califórnia). Para obter mais informações, consulte Regiões da AWS e Endpoints no Referência geral da AWS.	21 de dezembro de 2016
Conteúdo novo e atualizado	Esta versão adiciona suporte para a AWS Config região da Europa (Londres). Para obter mais informaçõ es, consulte Regiões da AWS e Endpoints no Referência geral da AWS.	13 de dezembro de 2016

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão adiciona suporte para a AWS Config região do Canadá (Central). Para obter mais informaçõ es, consulte Regiões da AWS e Endpoints no Referência geral da AWS.	8 de dezembro de 2016
AWS Config suporta os tipos de recursos do Amazon Redshift e duas novas regras gerenciad as	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seus clusters do Amazon Redshift, grupos de parâmetros de cluster, grupos de segurança de cluster, snapshots de cluster, grupos de sub-redes de cluster e assinaturas de eventos. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão oferece suporte a duas novas regras gerenciadas: • redshift-cluster-configuration-check • redshift-cluster-maintenanc esettings-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	7 de dezembro de 2016

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão adiciona suporte para uma nova regra gerenciada: • dynamodb-throughput-limit-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	7 de dezembro de 2016
Conteúdo novo e atualizado	Esta versão inclui o suporte para a criação de até 50 regras por região em uma conta. Para obter mais informações, consulte Limites do AWS Config na Referência geral da AWS.	7 de dezembro de 2016

Alteração	Descrição	Data de lançamento
AWS Config suporta o tipo de recurso de inventário de instâncias gerenciadas para o Amazon EC2 Systems Manager e três novas regras gerenciadas	Com essa versão, você pode usar AWS Config para registrar alteraçõe s na configuração do software em suas instâncias gerenciadas com suporte para inventário de instâncias gerenciadas. Para ter mais informações, consulte Recording Software Configuration for Managed Instances. Esta versão oferece suporte a três novas regras gerenciadas: • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applica tions-required • ec2-managedinstance-platform-check Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	1° de dezembro de 2016

Alteração	Descrição	Data de lançamento
AWS Config suporta o recurso de bucket do Amazon S3 e duas novas regras gerenciadas	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em seus buckets do Amazon S3. Para ter mais informações, consulte Tipos de recursos compatíveis. Esta versão oferece suporte a duas novas regras gerenciadas: • s3-bucket-logging-enabled • s3-bucket-versioning-enabled Para ter mais informações, consulte AWS Config Regras gerenciadas.	18 de outubro de 2016
Conteúdo novo e atualizado	Esta versão adiciona suporte AWS Config e AWS Config regras na região Leste dos EUA (Ohio). Para obter mais informações, consulte Regiões da AWS e Endpoints no Referência geral da AWS.	17 de outubro de 2016

Alteração	Descrição	Data de lançamento
Regras gerenciadas novas e atualizadas	Esta atualização adiciona suporte a oito novas regras gerenciadas: • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted Você pode especificar vários valores de parâmetro para as seguintes regras: • desired-instance-tenancy • required-tags Para ter mais informações, consulte Lista de regras AWS Config gerenciadas.	4 de outubro de 2016

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado para o AWS Config console	Essa atualização adiciona suporte à visualização AWS CloudTrail da atividade da API na AWS Config linha do tempo. Se CloudTrail estiver fazendo login na sua conta, você pode visualizar a criação, a atualizaç ão e a exclusão de eventos de API para alterações de configuração em seus recursos. Para ter mais informações, consulte Visualizando o histórico de configuração e conformid ade.	06 de setembro de 2016
AWS Config suporta o tipo de recurso do Elastic Load Balancing	Com essa versão, você pode usar AWS Config para registrar alteraçõe s de configuração nos balanceadores de carga do aplicativo Elastic Load Balancing. Para ter mais informaçõ es, consulte Tipos de recursos compatíveis.	31 de agosto de 2016
Conteúdo novo e atualizado	Esta versão adiciona suporte AWS Config às regras nas regiões Ásia-Pacífico (Cingapura) e Ásia-Pacífico (Sydney). Para obter mais informaçõ es, consulte Regiões da AWS e endpoints no Referência geral da AWS.	18 de agosto de 2016

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado para AWS Config as Regras	Esta atualização adiciona suporte para a criação de uma regra que possa ser acionada tanto pelas alterações de configuração como a uma frequência periódica da sua preferência. Para ter mais informaçõ es, consulte Modo de avaliação e tipos de gatilho para AWS Config regras. Esta atualização também adiciona suporte para você avaliar manualmente os seus recursos em relação às regras, e excluir resultado s da avaliação. Para ter mais informações, consulte Avaliando seus recursos com regras AWS Config. Esta atualização também adiciona suporte para avaliação adicional de outros tipos de recursos, com regras personalizadas. Para ter mais informações, consulte Avaliar tipos de recursos adicionais.	25 de julho de 2016

Alteração	Descrição	Data de lançamento
AWS Config oferece suporte aos tipos de recursos Amazon RDS e AWS Certificate Manager (ACM)	Com esta versão, você pode usar AWS Config para registrar alterações de configuração em suas instâncias de banco de dados do Amazon Relational Database Service (Amazon RDS), grupos de segurança de banco de dados, snapshots de banco de dados, grupos de sub-rede de banco de dados e assinaturas de eventos. Você também pode usar AWS Config para registrar alteraçõe s de configuração nos certificados fornecidos pelo ACM. Para ter mais informações, consulte Tipos de recursos compatíveis.	21 de julho de 2016
Informaçõ es atualizad as sobre o gerenciamento do gravador de configuração	Esta atualização adiciona etapas para renomear e excluir o gravador de configuração em Gerenciar o gravador de configurações.	07 de julho de 2016

Alteração	Descrição	Data de lançamento
Criação simplificada de funções e políticas atualizadas	Com essa atualização, a criação de uma função do IAM para AWS Config é simplificada. Esse aprimoramento está disponível nas regiões que têm suporte a regras do Config. Para oferecer suporte a esse aprimoramento, as etapas Configurando AWS Config com o console estão atualizadas, o exemplo de política em Permissões para o bucket Amazon S3 para o AWS Config canal de entrega está atualizado, e o exemplo de política em Exemplos de políticas baseadas em identidade para AWS Config está atualizado.	31 de março de 2016
Exemplo de funções e eventos para regras de Config	Esta atualização fornece exemplos de funções atualizadas em Exemplo de AWS Lambda funções para AWS Config regras (Node.js), e inclui exemplos de eventos em Eventos de exemplo para regras AWS Config.	29 de março de 2016
AWS Config GitHub Repositório de regras	Essa atualização adiciona informações sobre o GitHub repositório de AWS Config regras aoAvaliação de recursos com regras AWS Config. Esse repositório fornece exemplos de funções para regras personalizadas que são desenvolvidas e contribuídas pelos AWS Config usuários.	1 de março de 2016

Alteração	Descrição	Data de lançamento
AWS Config Regras	Esta versão apresenta as AWS Config regras. Com regras, você pode usar AWS Config para avaliar se seus AWS recursos estão em conformidade com as configurações desejadas. Para ter mais informaçõ es, consulte Avaliação de recursos com regras AWS Config.	18 de dezembro de 2015
AWS Config suporta tipos de recursos do IAM	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seus usuários, grupos, funções e políticas gerenciad as pelo cliente do IAM. Para ter mais informações, consulte Tipos de recursos compatíveis.	10 de dezembro de 2015
AWS Config suporta host dedicado EC2	Com esta versão, você pode usar AWS Config para registrar alteraçõe s de configuração em seus hosts dedicados do EC2. Para ter mais informações, consulte Tipos de recursos compatíveis.	23 de novembro de 2015

Alteração	Descrição	Data de lançamento
Informações de permissões atualizadas	Essa atualização adiciona informações sobre as seguintes políticas AWS gerenciadas para AWS Config: • `AWS_ConfigRole` : concede permissão ao AWS Config para obter detalhes de configuração sobre os recursos. Para ter mais informações, consulte Política de perfil do IAM para obter detalhes de configuração. • `AWSConfigUserAccess` — Concede acesso somente de leitura a um AWS Config usuário. Para ter mais informações, consulte Acesso somente para leitura a AWS Config.	19 de outubro de 2015
AWS Config Pré-visualização das regras	Esta versão apresenta a prévia das AWS Config Regras. Com regras, você pode usar AWS Config para avaliar se seus AWS recursos estão em conformidade com as configurações desejadas. Para ter mais informações, consulte Avaliação de recursos com regras AWS Config.	7 de outubro de 2015
Conteúdo novo e atualizado	Esta versão adiciona a capacidade de pesquisar recursos que AWS Config foram descobertos. Para ter mais informações, consulte Pesquisando recursos que são descobertos por AWS Config.	27 de agosto de 2015

Alteração	Descrição	Data de lançamento
Conteúdo novo e atualizado	Esta versão adiciona a capacidade de selecionar quais tipos de recursos o AWS Config registra. Para ter mais informações, consulte AWS Recursos de gravação.	23 de junho de 2015
Conteúdo novo e atualizado	Esta versão adiciona suporte para as seguintes regiões: Ásia-Pacífico (Tóquio), Ásia-Pacífico (Singapur a), Europa (Frankfurt), América do Sul (São Paulo) e Oeste dos EUA (Norte da Califórnia). Para obter mais informações, consulte Regiões da AWS e endpoints.	6 de abril de 2015
Novo guia	Essa versão apresenta o AWS Config.	12 de novembro de 2014

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.